СЛУЖБА БЕЗПЕКИ УКРАЇНИ
ІНСТИТУТ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАЦІОНАЛЬНОГО ЮРИДИЧНОГО УНІВЕРСИТЕТУ
ІМЕНІ ЯРОСЛАВА МУДРОГО

СБУ В УМОВАХ ВІЙНИ В УКРАЇНІ: СУЧАСНІ РЕАЛІЇ ТА ІННОВАЦІЙНІ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Матеріали міжнародної науково-практичної конференції 4–5 липня 2024 року

ПРАВОВА ЄДНІСТЬ
РЕДАКЦІЯ ЮРИДИЧНИХ ВИДАНЬ

Київ • Алерта • 2024

УДК 343.337
С23

Рекомендовано до видання
Вченою радою Інституту Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого
(протокол № 32 від 1 липня 2024 року)

С23 СБУ в умовах війни в Україні: сучасні реалії та інноваційні стратегії забезпечення національної безпеки: матеріали міжнародної науково-практичної конференції 4-5 липня 2024 року. Київ : Алерта, 2024. 298 с.

ISBN 978-617-566-847-4

У збірнику представлено матеріали міжнародної науково-практичної конференції 4-5 липня 2024 року, присвяченої обговоренню та вирішенню низки проблемних питань, пов'язаних з сучасними реаліями та інноваційними стратегіями забезпечення національної безпеки України в умовах триваючої війни. Зокрема тези виступів стосуються імплементації норм міжнародного гуманітарного права як контексту ефективного розслідування особливо небезпечних злочинів; сучасної парадигми контррозвідувальної та оперативно-розшукової діяльності; посилення спроможностей СБУ з розслідування злочинів, пов'язаних з розповсюдженням та застосуванням радіаційної, хімічної, біологічної та ядерної зброї; особливостям суспільно небезпечних посягань на інформаційну безпеку держави, зокрема сучасних умов розслідування та протидії; стану, викликів та майбутнього аналітичної розвідувальної діяльності.

Видання адресоване співробітникам практичних підрозділів СБУ, працівникам прокуратури, суду, науковим працівникам, аспірантам, викладачам закладів вищої юридичної освіти (факультетів ЗВО), а також іншим особам, до предмету зацікавленості яких відносяться порушені теми.

Редакційна колегія вважає за доцільне повідомити, що не всі положення і висновки окремих авторів є безперечними. Разом з тим, їх публікація здійснюється з метою забезпечення плюралізму наукової думки і публічного обговорення.

Матеріали друкуються мовою оригіналу. За виклад, зміст і достовірність матеріалів, а також використання наукових джерел без відповідного посилання відповідають автори.

УДК 343.337

ISBN 978-617-566-847-4

ЗМІСТ

СЕКЦІЯ 1
ІМПЛЕМЕНТАЦІЯ НОРМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА ЯК КОНТЕКСТ ЕФЕКТИВНОГО РОЗСЛІДУВАННЯ ОСОБЛИВО НЕБЕЗПЕЧНИХ ЗЛОЧИНІВ

СЕКЦІЯ 2
СУЧАСНА ПАРАДИГМА КОНТРРОЗВІДУВАЛЬНОЇ ТА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

СЕКЦІЯ 3
ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ СБУ З РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З РОЗПОВСЮДЖЕННЯМ ТА ЗАСТОСУВАННЯМ РАДІАЦІЙНОЇ, ХІМІЧНОЇ, БІОЛОГІЧНОЇ ТА ЯДЕРНОЇ ЗБРОЇ

СЕКЦІЯ 4
ОСОБЛИВО НЕБЕЗПЕЧНІ ПОСЯГАННЯ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ: СУЧАСНІ УМОВИ, РОЗСЛІДУВАННЯ, ПРОТИДІЯ

СЕКЦІЯ 5
АНАЛІТИЧНА РОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ: СТАН, ВИКЛИКИ ТА МАЙБУТНЄ

Секція 1
ІМПЛЕМЕНТАЦІЯ НОРМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА ЯК КОНТЕКСТ ЕФЕКТИВНОГО РОЗСЛІДУВАННЯ ОСОБЛИВО НЕБЕЗПЕЧНИХ ЗЛОЧИНІВ

РОЛЬ ПОЛІЦЕЙСЬКИХ ПРИ РЕАГУВАННІ НА ВОЄННІ ЗЛОЧИНИ НА ДЕОКУПОВАНИХ ТЕРИТОРІЯХ

Іван ВИГІВСЬКИЙ
кандидат юридичних наук,
співробітник Національної поліції України

Забезпечення безпеки особи, суспільства та держави від загроз злочинних посягань – найбільш пріоритетне завдання всіх інститутів державної влади в Україні, а в умовах збройного конфлікту безпекові ініціативи є важливим елементом в архітектурі безпекового середовища. З 24 лютого 2022 року Україна зіткнулася зі збройною агресією російської федерації, унаслідок якої відносно цивільних осіб і військовослужбовців вчиняються кримінальні протиправні діяння, значна частина яких складає воєнні злочини.

Відповідно до Стратегії воєнної безпеки України така безпека є однією із засадничих умов реалізації права українського народу на самовизначення, збереження держави Україна та забезпечення її сталого розвитку на основі найвищих цінностей демократії, верховенства права, свободи, гідності, безпеки і процвітання громадян усіх національностей. Захист суверенітету і територіальної цілісності України – найважливіша функція держави, справа всього українського народу [1]. Виявлення та збір доказів і повідомлення про воєнні злочини є критично важливою складовою міжнародних зусиль, спрямованих на запобігання та покарання за звірства, вчинені у збройних конфліктах. З початку повномасштабної війни Національна поліція України (далі – НПУ), крім завдань з охорони публічної безпеки та порядку, протидії злочинності та охорони прав і свобод людини, а також інтересів суспільства і держави, бере активну участь у виконанні завдань територіальної оборони, забезпеченні та здійсненні заходів правового режиму воєнного стану.

Для того, щоб поліцейські могли виконувати завдання, що пов'язані з доказами ймовірних воєнних злочинів, їх потрібно належним чином навчити правильним процесуальним діям. Вони також повинні мати можливість приділяти достатньо часу цим завданням, а не іншим поточним військовим операціям. Під час збройного конфлікту ресурсів завжди вкрай мало, а відповідного рівня підготовка щодо належного збору доказів займає дуже багато часу. Тому важливо ретельно продумати, виконання яких завдань можна очікувати від поліцейських у зв'язку з цим, і наскільки їх залучення є необхідним, корисним та ефективним. Таким чином, у більшості випадків слід очікувати, що поліцейські виконуватимуть максимальний обсяг завдань щодо виявлення потенційних воєнних злочинів. Прикладами можуть бути оповіщення відповідних органів; збереження місць та доказів воєнних злочинів, збір інформації про потенційних свідків або злочинців [2].

У рамках кожного кримінального провадження створюється міжвідомча слідча група, передусім Служби безпеки України та НПУ, до якої включаються слідчі центральних апа-

ратів, обласних управлінь (обох вказаних відомств), а також територіальних підрозділів поліції.

З метою забезпечення стійкої роботи Головних управлінь НПУ та міжрегіональних територіальних підрозділів, їх структурних та підпорядкованих (відокремлених) підрозділів при розслідуванні воєнних злочинів, а також з метою забезпечення публічного порядку і безпеки, протидії злочинності, надання якісних поліцейських послуг, забезпечення безпеки особового складу поліції під час відключень електроенергії, опалення та зв'язку плануються та здійснюються такі заходи: 1) підготовка плану першочергових дій особового складу у разі відключення енергопостачання, опалення та зв'язку; 2) розроблення схеми оповіщення особового складу на випадок втрати звичних джерел зв'язку внаслідок відключення енергопостачання; 3) визначення місця збору підпорядкованих працівників та шляхів їх прибуття (за необхідності – підвозу) до визначених місць; 4) проведення розрахунків сил та засобів, необхідних для забезпечення публічної безпеки і порядку, протидії злочинності, у разі відключення енергопостачання, опалення та зв'язку (з урахуванням підпорядкування особового складу відокремлених територіальних підрозділів міжрегіональних територіальних органів поліції начальникам ГУНП); 5) визначення чисельності та місць встановлення нарядів поліції, розроблення схем їх розташування на автошляхах державного та місцевого значення з метою забезпечення безпеки дорожнього руху і надання допомоги громадянам під час їх евакуації з великих населених пунктів у разі відключення енергопостачання, а також з урахуванням ускладнення погодних умов; 6) розроблення оперативних планів охорони важливих соціальних, фінансових, адміністративних будівель, об'єктів критичної інфраструктури, життєдіяльності населення тощо на випадок відключення енергопостачання, проведення розрахунків додаткового залучення сил та засобів поліції охорони для посилення охорони об'єктів, які охороняються інженерно-технічними засобами охорони з метою виставлення фізичної охорони на таких об'єктах; 7) отримання в ДСНС списків місць розташування пунктів незламності, пунктів обігріву, здійснення розрахунків особового складу, необхідного для забезпечення охорони публічного порядку в місцях їх розташування, а також доведення списків таких місць до кожного працівника поліції, які будуть нести службу у складі нарядів; 8) визначення місць (зон загального доступу) можливого розміщення у приміщеннях територіальних підрозділів поліції осіб, які потребуватимуть допомоги (обігріву, доступу до Інтернету тощо); 9) налагодження контактів з представниками комунальних служб з метою забезпечення відповідної співпраці в разі відключення енергопостачання або суттєвого ускладнення погодних умов; 10) вихід з клопотанням (за потреби) до відповідних військових адміністрацій про виділення додаткових сил і засобів для охорони публічного порядку і безпеки, охорони об'єктів (з числа територіальної оборони, добровольчих формувань територіальних громад, муніципальної варти тощо); 11) попередження особового складу про необхідність передбачення можливих варіантів переміщення сімей за межі великих міст до населених пунктів, де є індивідуальне опалення та можливість приготування їжі з розрахунку строком на 7–10 днів;

Робота поліцейських та інших залучених фахівців із фіксації та розслідування воєнних злочинів розпочинається на деокупованих територіях після закінчення заходів із їх розмінування, а також фільтраційних заходів (виявлення ДРГ, колаборантів, тощо).

У рамках роботи Координаційного штабу вирішуються питання залучення необхідних, у тому числі додаткових, сил та засобів для забезпечення ефективної роботи. Крім того, у рамках штабу забезпечується накопичення, своєчасний обмін, систематизація та аналіз інформації про результати відпрацювання територій та розслідування злочинів, планування подальшої роботи тощо.

Під час проведення слідчих дій у кримінальних провадженнях необхідно ефективно розподіляти задачі між слідчими різних органів в залежності від їх звичної спеціалізації. Зокрема, слідчим органів НПУ необхідно зосередити увагу на фіксації та розслідуванні: вбивств; обставин масових захоронень; сексуального насильства; жорстокого поводження із цивільним населенням; обставин функціонування місць масового незаконного утримання цивільного насе-

лення, жорстокого поводження із ним; фактів безвісного зникнення на окупованих територіях; незаконного позбавлення волі; розграбування майна; нападів на цивільні об'єкти.

Наприклад, огляд місця події за фактами воєнних злочинів, зокрема обстрілів або вибухів є найскладнішим видом слідчого огляду, важливою та невідкладною СРД, яку здійснюють на підставах і в порядку, передбачених ст. 214, 237, 238 КПК України [3]. Метою огляду за фактами обстрілів або вибухів є фіксація наслідків руйнувань рухомих і нерухомих об'єктів, місцевості, місць загибелі людей, факту застосування засобів ведення війни, заборонених міжнародним правом, задля подальшої ідентифікації загиблих, встановлення завданих збитків, виявлення та вилучення предметів (залишків снарядів, мін тощо), зокрема заборонених міжнародним правом, які призвели до загибелі людей та руйнувань, безпечне переміщення таких предметів до визначених місць для зберігання як речових доказів, а також їх знищення в разі необхідності.

Завданнями огляду за фактами обстрілів або вибухів є: фіксація порушення законів і звичаїв війни – визначення місця вчинення злочину, дати й часу, встановлення можливого засобу ураження; визначення типу засобу ураження (дослідження залишених вирв і залишків боєприпасів); з'ясування напрямку стрільби (за конфігурацією вирв і розльоту залишків боєприпасів створюють схему відтворення); встановлення можливого району знаходження засобу ураження (за напрямком стрільби визначають можливий район знаходження засобу вогневого ураження (2/3 максимальної дальності стрільби), досліджують космічні знімки району).

Серед особливостей огляду та вилучення об'єктів з місця обстрілу (вибуху) можна виокремити такі: проведення аварійно-рятувальних робіт; велика площа обстеження та кількість слідів, зокрема фрагментів боєприпасів чи вибухових пристроїв, переважно невеликих за розмірами; значна кількість фрагментів речової обстановки, які ускладнюють виявлення залишків боєприпасів чи вибухових пристроїв; наявність потерпілих, яким потрібне надання медичної допомоги й евакуація; несприятливі погодні умови (під час огляду на відкритій місцевості); потрапляння під повторний обстріл, можливість вибухів додаткових боєприпасів чи вибухових пристроїв і легкозаймистих речовин, обвалів, пожеж й інших факторів, небезпечних для здоров'я та життя людини, тощо; складання протоколу огляду поза межами місця події, з використанням матеріалів фото-, відеозапису, планів-схем, чернеток і нотаток, створених, зокрема, з використанням аудіо- та відеозаписувальних пристроїв на місці події; дотримання заходів безпеки під час виявлення, огляду, вилучення, транспортування та зберігання вилучених вибухонебезпечних речових доказів [4, с. 94].

Таким чином, діяльність органів і підрозділів НПУ під час реагування на воєнні злочини на деокупованих територіях спрямована на забезпечення швидкого, повного та неупередженого розслідування з тим, щоб кожний, хто вчинив такі кримінальні протиправні діяння на території України був притягнутий до відповідальності в міру своєї вини

Список використаних джерел:

1. Стратегія воєнної безпеки України: Указ Президента України від 25.03.2021 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021–37661. (дата звернення: 15.06.2024).

2. Роль правоохоронних органів у реагуванні на воєнні злочини / Г. Ясутіс, Р. Мікова, Д. Прескотт, В. Шабас. Женевський центр з управління сектором безпеки. Женева, 2024. 33 с.

3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. URL: http://zakon3.rada.gov.ua/laws/show/4651–17. (дата звернення: 15.06.2024)

4. Кваліфікація та розслідування порушення законів і звичаїв війни: наук.-практ. посіб. / А.А. Вознюк, І.В. Жук, О.В. Таран, С.С. Чернявський та ін.; за заг. ред. В.В. Чернєя, М.С. Цуцкіридзе, А.А. Вознюка. Київ: Норма права, 2023. 326 с.

КЕРУВАННЯ ТА КОНТРОЛЬ ЗА ПОЛІТИЧНИМИ ЧИ ВІЙСЬКОВИМИ ДІЯМИ ДЕРЖАВИ ЯК ОЗНАКА СПЕЦІАЛЬНОГО СУБ'ЄКТА ЗЛОЧИНУ АГРЕСІЇ

Валентин ГАРАЩУК
співробітник СБУ

Стаття 8bis частина 1 Римського статуту зазначено, що «злочин агресії» означає планування, підготовку, ініціювання або вчинення особою, яка спроможна фактично здійснювати контроль за політичними чи військовими діями держави або керувати ними, акту агресії, який за своїм характером, тяжкістю та масштабами є грубим порушенням Статуту Організації Об'єднаних Націй.

Це визначеня чітко окреслює ознаки спеціального суб'єкта міжнародної індивідуальної відповідальності за злочини агресії – особа, яка фактично здійснює контроль за політичними військовими діями держави або керує такими діями.

Проте Україна донині не ратифікувала цей міжнародний нормативно-правовий акт, а з урахуванням, що ст. 437 КК України безпосередньо не визначає ознаки, якими має бути наділений суб'єкт цього кримінального правопорушення, судова слідча практика має певну непослідовність у питанні кваліфікації суспільно небезпечних діянь за ознаками планування, підготовки, розв'язування та ведення агресивної війни.

Спроба законодавчого вирішення означеної проблеми була започаткована у Проекті Закону «Про внесення змін до деяких законодавчих актів України щодо імплементації норм міжнародного кримінального та гуманітарного права» № 2689 від 27.12.2019, що був прийнятий у другому читанні 20.05.2021. Стаття 437 Проекту (Злочин агресії) визначала, що за планування, підготовку, ініціювання або вчинення акту агресії несе кримінальну відповідальність особа, яка здатна фактично здійснювати контроль або керівництво політичними чи військовими діями держави [1]. Проте ці зміни не набули чинності.

Судово-слідча практика сьогодення у вирішенні питання щодо суб'єкта злочину передбаченого ст. 437 КК України базується на тому, що вичерпного переліку осіб, що потенційно можуть відповідати за злочин агресії не визначений, чим забезпечується можливість вирішення питання про те, чи є конкретна особа відповідальною за злочин агресії з огляду на контекст конкретної справи, зокрема особливості державного та суспільного устрою у відповідній країні.

Як наслідок, відповідальними за акт агресії в окремих випадках визнаються особи, що формально не займають будь-яких державних посад, проте, які спроможні здійснювати контроль та керувати військово-політичною діяльністю держави на найвищому рівні [2]; особи які є командуючими окремими підрозділами збройних сил рф [3]; а в інших звичайні військовослужбовці збройних сил держави агресора [4].

Суди вважають, що з огляду на ті міжнародно-правові зобов'язання, які породжує для України безпосередня криміналізація агресії за міжнародним правом, кримінально-правова заборона цього типу поведінки за кримінальним законодавством України також повинна поширюватися лише на зазначених вище осіб. При цьому суди не вбачають переконливих підстав вважати, що положення ст. 437 КК поширюються на більш широке коло суб'єктів, оскільки ніщо у тексті зазначеної норми на це буквально не вказує.

Тому, зважаючи на міжнародно-правову ґенезу положень ст. 437 КК, суб'єкт планування, підготовки, розв'язування та ведення агресивної війни за кримінальним законодавством України, на думку суддів, є спеціальним, а саме – таким суб'єктом є особа, яка спроможна фактично здійснювати контроль за політичними чи військовими діями держави або керувати ними. Для того, щоб визначити, чи перебувала та чи інша особа під таким контролем, виправданим може

бути застосування стосовно груп осіб, організованих за воєнним принципом – критерію «загального контролю» (не просто постачання зброї, техніки чи фінансування, а координація державою військових операцій, внесення вкладу в загальне планування, нехай хоч і без віддання наказів про вчинення конкретних діянь), а стосовно фізичних осіб та груп, не організованих за воєнним принципом – критерію «ефективного контролю» (видача конкретних наказів, інструкцій) [2].

Для правильного та однакового застосування судами законодавства про відповідальність за злочин, передбачений ст. 437 КК України Велика Палата Верховного Суду, 28 лютого 2024 року у справі № 415/2182/20 (провадження № 13–15кс22) визначила, що це суспільно небезпечне діяння здатні вчиняти особи, які в силу службових повноважень або фактичного суспільного становища спроможні здійснювати ефективний контроль за політичними чи воєнними діями або керувати ними, та/або істотно впливати на політичні, військові, економічні, фінансові, інформаційні та інші процеси у власній державі чи за її межами, та/або керувати конкретними напрямами політичних або воєнних дій [5].

Висновки. Пунктом 3 ст. 24 «Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони» передбачено посилення взаємодії щодо взаємної правової допомоги та екстрадиції. Це включатиме, у разі необхідності, приєднання до відповідних міжнародних документів ООН та Ради Європи, зокрема Римського статуту Міжнародного кримінального суду 1998 року, та їх виконання, як зазначається у статті 8 цієї Угоди, а також більш тісне співробітництво з Євроюстом. Правова допомога є вкрай необхідною для України з огляду на невідворотність притягнення до кримінальної відповідальності осіб винних за розв'язування агресії проти нашою держави та вчинення воєнних злочинів на її території.

У свою чергу ефективність правової допомоги суттєво залежить від процесу адаптації законодавства України до законодавства ЄС. Ще 18 березня 2004 року Законом України була прийнята «Загальнодержавна програма адаптації законодавства України до законодавства європейського союзу» відповідно до якої було визначено механізм адаптації законодавства, утворення відповідних інституцій та інші додаткові заходи, необхідні для ефективного правотворення та правозастосування. Метою адаптації законодавства України до законодавства Європейського Союзу є досягнення відповідності правової системи України acquis communautaire з урахуванням критеріїв, що висуваються Європейським Союзом (ЄС) до держав, які мають намір вступити до нього. Цей процес є пріоритетною складовою процесу інтеграції України до Європейського Союзу.

А отже необхідне внесення змін до законодавства про кримінальну відповідальність в частині імплементації положень Римського статуту, яким визначено підстави відповідальності за злочин агресії.

Список використаних джерел:

1. Про внесення змін до деяких законодавчих актів України щодо імплементації норм міжнародного кримінального та гуманітарного права: проєкт закону 2689 від 27.12.2019 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67804(дата звернення: 20.06.2024).

2. Дніпровський районний суд м. Києва: вирок у справі № 1-кп/755/369/23 від 10.05.2023 URL: https://reyestr.court.gov.ua/Review/ 110758134. (дата звернення: 20.06.2024)

3. Бородянський районний суд Київської області: ухвала у справі № 1-кп/939/122/23 від 5 листопада 2023 року URL: https://reyestr.court.gov.1-кп/939/122/23 ua/Review/114929866. (дата звернення: 20.06.2024)

4. Вирок Дзержинського міського суду Донецької області: кримінальна справа № 225/6623/15-к URL: https://reyestr.court.gov.ua/ Review/58821642. (дата звернення: 20.06.2024)

5. https://yur-gazeta.com/golovna/velika-palata-verhovnogo-sudu-viznachila-oznaki-subekta-zlochinu-peredbachenogo-st-437-kk-ukrayini.html. (дата звернення: 20.06.2024)

ГЕНЕЗА ІМПЛЕМЕНТАЦІЇ НОРМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА В НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО

Ігор ЄВТУШЕНКО
кандидат юридичних наук,
завідувач кафедри Національного
юридичного університету
імені Ярослава Мудрого

Світовий досвід ведення воєн показує що в результаті порушення рівноваги суспільних відносин, виникають суперечності в суспільстві на різних рівнях (політичні, релігійні, етнічні тощо) і стають причинами виникнення різних за масштабами та тривалістю збройних конфліктів що може призводити до переростання у воєнні дії та воєнні конфлікти. Каталізаторами таких явищ можуть бути різні обставини в суспільстві, наприклад, масові заворушення, революції, перевороти, акти тероризму тощо. Також, не лишаються осторонь і глобалізаційні процеси, які мають геополітичний вплив на зародження й розвиток збройного конфлікту. [2]

Як результат проведення кровопролитних воєн у XX сторіччі стало об'єднання лідерів провідних країн Світу та утворення безпекових організацій направлених на формування та запровадження Статутів, Декларацій та Конвенцій, метою створення котрих було убезпечення цивілізованого світу від кровопролитних воєн та від знищення цивілізацій. Результатом стало формування загальної нормативної бази міжнародного гуманітарного права як самостійної галузі міжнародного права.

Міжнародне гуманітарне право (далі – МГП) (право збройних конфліктів) – система міжнародно визнаних правових норм і принципів, що застосовуються під час збройних конфліктів, встановлюють права і обов'язки суб'єктів міжнародного права щодо заборони чи обмеження використання певних засобів і методів ведення збройної боротьби, забезпечення захисту жертв конфлікту та визначають відповідальність за порушення цих норм. [3]

Однак, сучасна практика реагування на кризові ситуації показала що сучасні збройні конфлікти та війни потребують комплексного вирішення, а також участі владних структур та Світових безпекових організацій в захисті громадян, конституційного ладу, суверенітету та територіальної цілісності держави. Також, як показала подальша практика та світовий досвід нових кровопролитних воєн, потребує додаткового контролю за додержанням норм МГП, в тому числі і шляхом імплементації цих норм в національному законодавстві держав, які ратифікували їх та зобов'язались дотримуватись.

На думку Доді К.В., імплементація міжнародного гуманітарного права на національному рівні потребує вирішення питання співвідношення норм міжнародного права з нормами внутрішнього. Національна правова система стосовно імплементації норм міжнародного права в тому числі і міжнародного гуманітарного права внутрішнє законодавство має особливості, зумовлені, конституційними нормами, які відповідно до положень Конституції України в першу чергу забезпечують пріоритетність та незалежність національного законодавства. [1]

Так, в ході розвитку незалежної держави України, на законодавчому рівні здійснювались кроки щодо імплементації норм МГП в національному законодавстві України. Як приклад 24 вересня 1993 року було між Україною, російською федерацією та білоруссю було підписано Угоду про першочергові заходи стосовно захисту жертв збройних конфліктів, нормами якої сторони зобов'язались співпрацювати та запобігати порушенню прав людини й норм гуманітарного права, зобов'язались привести національне законодавство у відповідність до норм МГП та в статті 6 зобов'язались що кожен з підписантів вживе всіх необхідних заходів для припинення будь-яких дій, що порушують МГП, зокрема застосування ефективних заходів

судового переслідування та покарання до осіб, які організували, учинили або наказали вчинити діяння, що кваліфікується як військовий злочин або злочин людства за міжнародним правом та (або) національним законодавством. Проте, як ми бачимо, російська федерація свідомо та агресивно порушує власні зобов'язання. [4]

Наступним кроком по імплементації норм МГП в національному законодавстві стало запровадження наказу Міністра Оборони України від 11 вересня 2004 року № 400 «Про затвердження Керівництва по застосуванню норм міжнародного гуманітарного права в Збройних Силах України».

На наступному етапі подій в державі спостерігались способи російської федерації зашкодити державному суверенітету України, територіальній цілісності та Конституційному ладу шляхом застосування гібридних форм і методів, які не підпадали під норми МГП та національного законодавства, що ускладнювало, а місцями унеможливлювало належне реагування на виклики та протидіяти їм як в площині національного законодавства так і за допомогою залучення Світових безпекових організацій.

Як результат, наукова спільнота [5, 6, 7] визначила появу у міжнародному гуманітарному праві застосування чотирьох типів збройних конфліктів: міжнародні збройні конфлікти, учасниками яких можуть бути держави та їх об'єднання (міжнародні організації); визвольні війни і війни за самовизначення, у яких народи ведуть боротьбу проти колоніального панування, іноземної окупації та проти расистських режимів; збройні конфлікти неміжнародного характеру, що не мають міжнародного характеру і виникли на території однієї з держав; збройні конфлікти неміжнародного характеру, що відбуваються на території будь-якої з держав між його збройними силами й антиурядовими збройними силами або іншими організованими збройними групами, які, перебуваючи під відповідальним командуванням, здійснюють такий контроль над частиною її території, який дозволяє їм здійснювати безперервні й узгоджені воєнні дії. [2]

Всі перелічені події примусили адаптуватись Україну до таких умов та активізували діяльність по удосконаленню національного законодавства і подальшого етапу імплементації норм МГП у тому числі і в кримінальному та кримінальному-процесуальному законодавстві. Так, у 2017 році було затверджено наказ Міністерства Оборони України від 02 березня 2017 року № 164 «Про затвердження Інструкції про порядок виконання норм міжнародного гуманітарного права у Збройних Силах України», також цим же наказом було визнано таким що втратив чинність наказ Міністра Оборони України від 11 вересня 2004 року № 400. Крім того в період 2014–2018 роки змінювалось національне законодавство і в контексті формування єдиної концепції по захисту держави від «гібридної війни» та інших загроз державі з боку російської федерації та неурядових військових формувань, які діяли за посередництвом російської федерації. [8]

24 лютого 2022 року російська федерація розпочала широкомасштабну війну проти України у зв'язку із чим на території нашої держави було введено правовий режим воєнного стану. Країна-агресор в межах широкомасштабної війни додатково застосовує різноманітні форми та методи ведення війни, виходячи за межі норм МГП. Що в свою чергу вимагає від представників органів державної влади та представників сил сектору безпеки і оборони продовжити шлях імплементації норм МГП в національному законодавстві для ефективної протидії країні-агресору та якісному формуванню доказової бази для подальшого представлення доказів Міжнародному кримінальному суду.

Одним з таких етапів подальшої імплементації є підготовка Проєкта Закону про міжнародні оборонні компанії, який визначає правовий статус та організаційно-правові засади діяльності міжнародних оборонних компаній, які створюються в Украйні та беруть участь у здійсненні оборонних заходів та надають за межами території Украйни оборонні послуги. [4]

Список використаних джерел:

1. Конституція України від 28 червня 1996 р. // Офіційний Вісник України. 1996. № 30. Ст. 141.;

2. Бєлай С., Євтушенко І. «ОСОБЛИВОСТІ ВЗАЄМОДІЇ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ.» // Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд в майбутнє / Матеріали панельної дискусії VII Харківського Міжнародного юридичного форуму / Редакційна колегія (2023): 12.;

3. Наказ Міністерства Оборони України від 02 березня 2017 року № 164 «Про затвердження Інструкції про порядок виконання норм міжнародного гуманітарного права у Збройних Силах України»;

4. Угода про першочергові заходи стосовно захисту жертв збройних конфліктів від 24 вересня 1993 р. URL https://zakon.rada.gov.ua/laws/show/997_037#Text (дата звернення: 15.06.2024);

5. Гібридизація безпекового середовища на теренах Східної Європи та пострадянського простору. Інформація, аналітика, огляди. Львів: Центр міжнародної безпеки та партнерства, 2016. Вип. 2. С. 2–3. URL: http://www.ispc.org.ua (дата звернення: 15.06.2024);

6. Кузніченко С.О. Адміністративно-правовий режим воєнного стану: монографія. Харків: Право, 2014. 232 с.;

7. Levchyk V. Hybrid war against Ukraine and NANO response. Безпека & партнерство: інформ.– аналіт. бюл. Львів: Центр міжнародної безпеки та партнерства, 2015. Вип. 1. С. 3–6.;

8. Базов В.П. Принципи міжнародного гуманітарного права // Юридична Україна. 2020. № 12 / DOI 10.37749/2308–9636–2020–12(216)-4. URL: http://yu.yurincom.com/wp-content/uploads/2021/05/pdf-67.pdf (дата звернення: 16.06.2024).

КВАЛІФІКАЦІЯ СУСПІЛЬНО НЕБЕЗПЕЧНИХ ДІЯНЬ ЗА ОЗНАКАМИ ВИКОРИСТАННЯ ЦИВІЛЬНОГО НАСЕЛЕННЯ ЯК «ЖИВИХ ЩИТІВ»

Сергій КЛИМЕНКО
кандидат юридичних наук, доцент,
співробітник СБУ
Олексій ІСКРЮК
співробітник СБУ

Під час збройної агресії рф проти України все частіше спостерігається тенденція, коли збройні сили рф діють зсередини густонаселених районів, таких як села, містечка та міста, і розміщують свої військові об'єкти поблизу перебування цивільних осіб та об'єктів. Розташовуючи військові об'єкти в місцях великого скупчення цивільного населення, рф прагне використовувати цивільних осіб та об'єкти для перешкоджання військовим діям ЗСУ. Ця тактика, відома в міжнародному гуманітарному праві як використання живих щитів, метою якої є створення правового бар'єру, адже у більшості випадків напад на такі військові об'єкти буде забороненим, якщо як очікується, такий напад призведе до непропорційних втрат серед цивільного населення.

У доповіді Незалежної міжнародної комісії з розслідування порушень в Україні під час збройної агресії російські збройні сили у 2022–2023 р. наражали цивільне населення на значні ризики. Комісія встановила, що вони неодноразово навмисно розміщували свої війська або техніку в житлових районах, а іноді змушували цивільне населення залишатися там або поблизу їхніх позицій [1].

Використання «живих щитів» є незаконним методом ведення війни, заборона якого передбачена низкою міжнародних нормативно правових актів серед яких: Додатковий протокол I [2] де у п. 7 ст. 51 передбачено, що присутність або пересування цивільного населення або ок-

ремих цивільних осіб не повинні використовуватись для захисту певних пунктів або районів від воєнних дій, зокрема у спробах захистити воєнні об'єкти від нападу або прикрити воєнні дії, сприяти чи перешкодити їм. Сторони, що перебувають у конфлікті, не повинні направляти пересування цивільного населення або окремих цивільних осіб з метою спробувати захистити воєнні об'єкти від нападу чи прикрити воєнні операції; ст. 28 Женевської конвенції IV (1949) [3], яка зазначає, що не може бути використано присутність будь-якої особи, яка перебуває під захистом, у будь-яких пунктах чи районах для захисту цих місць від воєнних операцій.

Поняття «живі щити» застосовується до цивільних чи інших осіб, що знаходяться під захистом міжнародного гуманітарного права, чия присутність або пересування спрямовані на те, щоб захистити військові цілі від нападу супротивника. Тактика застосування живих щитів в залежності від ситуації різниця і може полягати, як у використанні присутності цивільного населення поблизу військового об'єкту, так і в безпосередньому залученні цивільних осіб до операцій наступального чи оборонного характеру. При цьому цивільне населення може виступати в якості «живого щита» як добровільно, так і під примусом.

Найбільш дискусійним у теорії міжнародного гуманітарного права сьогодні є питання використання «добровільних живих щитів». Це пов'язано з тим, що в чинних міжнародних нормативно-правових актах ця ситуація не регламентується. У національній юридичній літературі це питання не будо предметом наукового дослідження, утім було предметом розвідок зарубіжних вчених, таких як Homayon Habibi, Salehe Ramezani, Amichai Cohen, David Zlotogorski, Bence Kis Keleman та ін.

Деякі вчені вважають, добровільний «живий щит» передбачає безпосередню участь цивільних осіб у бойових діях, що позбавляє їх захисту, яку МГП надає цивільним особам. Проте думка опонентів відкидає цю інтерпретацію [4].

На зустрічі експертів з поняттям безпосередньої участі в бойових діях, що відбулося в м. Гаага, 25/26 жовтня 2004 р. не вдалося виробити спільну позицію щодо того, за яких обставин дії як «живий щит» будуть становити безпосередню участь у військових діях [5].

Водночас експертами було зазначено, що військовий об'єкт, навіть будучи оточений цивільними особами, продовжує залишатися військовою ціллю, і напад на нього буде незаконним тільки у разі, якщо передбачуваний непрямий збиток буде надмірним відносно конкретної і прямої військової переваги, яка має бути отриманою.

Той факт, що окремі цивільні особи добровільно і навмисно зловживають своїм юридичним правом на захист для відвернення нападу на військовий об'єкт, не тягне за собою втрати належного їм права на захист і не дає права нападати безпосередньо на них, яким би об'єкт ними не прикривався.

Відповідно до положення п. (b) (xxiii) ч. 2 ст. 8 Римського статуту – використання присутності цивільної особи або іншої особи, яка перебуває під захистом, для захисту певних пунктів, районів або збройних сил від військових операцій визнається воєнним злочином [6].

У судовій практиці є чисельні випадки засудження воєнних злочинців за використання «живих щитів» як методу ведення війни. Так, у справі Радована Караджича, розглянутій Міжнародним кримінальним трибуналом для колишньої Югославії (МКТЮ), Р. Караджич був визнаний винним у численних воєнних злочинах, злочинах проти людяності та геноциді. Серед інших звинувачень, він був визнаний винним у використанні цивільних осіб як живих щитів. Це було частиною тактики, яку використовували боснійські серби під його керівництвом під час конфлікту в Боснії і Герцеговині. Суд визнав, що між 26 травня і 2 червня 1995 року боснійські сербські військові під керівництвом Р. Караджича та Ратко Младича захопили миротворців ООН і використовували їх як живі щити, розміщуючи їх на військових об'єктах для захисту від нападів збройних сил НАТО. Це було зроблено з метою перешкодити авіаударам НАТО по боснійсько-сербських позиціях [7].

Стаття 438 КК України (порушення законів і звичаїв війни) не містить на відміну від положення ст. 8 Римського статуту МКС окремо визначеної форми суспільно небезпечного діяння, відповідно до якої здійснювалась б кваліфікація за використання цивільного населення

як «живого щита». Відсутня на сьогодні і судова практика, яка б могла дати певні правозастосовні орієнтири у цьому напрямку. З урахуванням форм суспільно небезпечного діяння відображених у чинній редакції даної кримінально-правової норми на нашу точку зору такі дії слід кваліфікувати як інші порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України.

Список використаних джерел:

1. Доповідь Незалежної міжнародної комісії з розслідування порушень в Україні Рада з прав людини П'ятдесят друга сесія 27 лютого – 31 березня 2023 Пункт 4 порядку денного Ситуації у сфері прав людини, що потребують уваги Ради Distr.: General 15 March 2023. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/coiukraine/A_HRC_52_62_UA.pdf. (дата звернення: 16.06.2024)

2. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року URL: https://zakon.rada.gov.ua/laws/show/995_199#Text. (дата звернення: 16.06.2024)

3. Женевська конвенція про захист цивільного населення під час війни від 12 серпня 1949 року URL: https://zakon.rada.gov.ua/laws/show/995_199#Text. (дата звернення: 16.06.2024)

4. Homayon Habibi, Salehe Ramezani. Legal Status of Voluntary Human Shield in International Humanitarian Law. FAṢLNĀMAH-I PIZHŪHISH-I HUQŪQ-I ʿUMŪMĪ (APR2015) Vol. 16, no. 45.pp. 77–103.

5. Second Expert Meeting Direct Participation in Hostilities under International Humanitarian Law. The Hague, 25–26 October 2004. Co-organized by the ICRC and the TMC Asser Institute URL: https://www.icrc.org/en/doc/assets/files/other/direct_participation_in_hostilities_2004_eng.pdf. (дата звернення: 16.06.2024)

6. Римський Статут Міжнародного кримінального Суду URL: https://zakon.rada.gov.ua/laws/show/995_588#Text. (дата звернення: 16.06.2024)

7. Trial Judgement Summary for Radovan Karadžić URL: https://www.icty.org/x/cases/karadzic/tjug/en/160324_judgement_summary.pdf. (дата звернення: 16.06.2024)

ДО ПИТАНЬ ВПРОВАДЖЕННЯ СТАНДАРТІВ НАТО У БЕЗПЕКОВЕ СЕРЕДОВИЩЕ УКРАЇНИ

Артемій КАПЕЛЮХА
співробітник СБУ

Сьогодні в рамках міжнародного співробітництва України з іноземними країнами відбувається залучення фінансової та технічної підтримки, обмін кращим міжнародним досвідом та приведення українських стандартів у відповідність до світових практик. Одним з основних завдань міжнародної співпраці є сприяння реформуванню та розвитку національних спецслужб для досягнення оперативної сумісності з відповідними підрозділами держав-членів НАТО та ЄС, впровадження стандартів НАТО у різні сфери діяльності безпекових структур, виконання відповідних критеріїв, необхідних для набуття членства України в НАТО. Міжнародне співробітництво з військової стандартизації орієнтовано на поглиблення співробітництва з державами-членами НАТО.

Ще у 2014 році було започатковано Програму посилених можливостей НАТО (ЕОР), яка сприяє розширенню співпраці партнерів з Альянсом, посиленню оперативної сумісності військ країн-учасниць Програми з силами НАТО. Тобто, чим вище ця сумісність, тим простіша і ефективніша участь військових підрозділів партнерів у місіях і операціях Альянсу. Кожній

з країн-партнерів НАТО було визначено пріоритети оборони. Зокрема, Україні – такі: досягти у максимально стислі строки взаємосумісності Збройних Сил та інших складових сектору безпеки і оборони з НАТО; суттєво активізувати реформи для досягнення відповідності критеріям членства в НАТО у рамках імплементації Річних національних програм; отримати запрошення та приєднатися до Плану дій щодо членства в НАТО [1].

Серед безлічі документів НАТО, близько 1200 стандартів, які спрямовані виключно на забезпечення досягнення оперативної і технічної сумісності сил оборони. Запровадження стандартів НАТО не гарантує набуття членства в Альянсі, а є лише однією з запорук на шляху до цього. Наприклад, Річні національні програми під егідою Комісії Україна-НАТО містять лише два розділи, присвячені оборонним, військовим і безпековим питанням. Усі інші розділи розкривають політичні, економічні, ресурсні та правові питання. У Річних національних програмах прописано механізми реалізації та втілення необхідних змін у всіх аспектах життя держави, що є ключовим інструментом інтеграції України до Альянсу і дорожньою картою реформ для втілення стандартів НАТО.

Одним зі способів прискорити запровадження стандартів НАТО є залучення науковців у сфері військових, юридичних та політичних наук до активної співпраці з профільними відомствами та парламентарями [2]. Тому саме акцентуємо на тематиці впровадження стандартів НАТО у безпекове середовище серед присутньої на заході наукової спільноти.

Проблемам адаптації національного законодавства до стандартів НАТО сьогодні приділяється багато уваги як в науковій так і в науково-популярній літературі. Окрім публікацій у журналах можна побачити багато веб-сайтів, інтернет-сторінок, що висвітлюють діяльність безпекових структур НАТО в Україні, в тому числі стандартизації. Так, О. Кривенко, досліджуючи проблеми розвитку системи військового законодавства та його адаптації до стандартів НАТО, дійшов наступних висновків: 1) розвиток законодавства у сфері оборони є складним системним процесом, який доцільно розглядати у трьох аспектах: теоретико – правовому, організаційно – правовому та в аспекті адаптації до стандартів НАТО; 2) ефективність заходів з розвитку законодавства у сфері оборони залежить від планової, системної та своєчасної роботи насамперед Ради національної безпеки і оборони України та Міністерства оборони України у жорсткій відповідності до Державної програми розвитку ЗС України та Програмами розвитку інших складових сектору оборони; 3) провідна роль у координації розвитку системи військового законодавства та його адаптації до стандартів Організації Північноатлантичного договору (НАТО) належить Раді національної безпеки і оборони України; 4) доцільно видати нормативно-правовий акт, який би комплексно врегульовував відповідальність, порядок і терміни розробки актів військового законодавства та його адаптації до стандартів НАТО [3, С. 34,35]. Є. Плешко, розглядаючи питання військової стандартизації, як єдиної мови та важливої умови взаємосумісності в НАТО, дійшов важливих висновків. Зокрема, виділимо наступні. По-перше, базова термінологія щодо стандартів НАТО досі має різне застосування, а тому одразу необхідно виключити питання, що стосуються комунікації та фасилітації військово-цивільного характеру. Але сфера безпеки і оборони вимагає єдності підходів та усталеного розуміння саме військової стандартизації, що без перебільшення є однією з найважливіших умов взаємосумісності в НАТО. По-друге, швидкість процесу переходу на стандарти НАТО до моменту, який дозволяє досягти взаємосумісності, у кожній країні свій. Наприклад, Литві знадобилося десять років, Чехія потребувала дев'яти років, а Польща впоралася за вісім років. Важливо розуміти, шо мова не йде про повну імплементацію усієї нормативної бази НАТО у сфері військової стандартизації. Варто врахувати, що жодна держава-член Альянсу не впровадила всіх стандартів НАТО, а у деяких частка впровадження сягає лише близько 25% від загальної кількості нормативних документів[4].

Крім того, слід мати на увазі, що близько 65% стандартизаційних угод НАТО (STANAGs – Standardization Agreements), які частіше називають стандартами, складають документи оперативного напряму, близько 20% – матеріальні та технічні документи, і близько 15% – адміністративні. При цьому кожні 3 роки усі стандарти переглядаються [5]. Але загалом, база даних

стандартів (NATO Standardization Documents Database. NSDD) налічує понад 2000 угод із стандартизації, об'єднаних в 43 функціональні групи, та понад 8000 інших документів Альянсу з питань стандартизації [6]. Система стандартів НАТО об'єднана у складну систему нормативних документів, що стосуються стандартизації. Серед них можна виділити: союзні стандарти: власне стандарти НАТО (А…Р – Allied Publications, М…Р – Multinational Publications) та стандарти окремих держав-членів НАТО; супровідні документи: угоди зі стандартизації (STANAG – Standardization Agreement) та рекомендації зі стандартизації (STANREC – Standardization Recommendation); інші документи, які пов'язані із стандартами (SRD – Standardization Related Documents). [7]

Слушною є думка очільника Управління стандартизації, кодифікації та каталогізації Міноборони України О. Кумеди про те, що стратегічними оборонними документами України передбачена взаємосумісність з військами/силами Альянсу та збройними силами держав-членів НАТО не лише Збройних Сил України, а й інших складових сил оборони (Служби безпеки України, Національної гвардії України, Державної прикордонної служби України тощо). Отже, доцільно розглядати необхідність запровадження в усіх інститутах сил оборони певного відсотка стандартів НАТО (до прикладу, з питань планування операцій, логістики, медичного забезпечення тощо), особливо тих, які передбачені Цілями партнерства [8].

Зрозуміло, що впровадження стандартів НАТО у безпекове середовище нашої країни – це складний, довготривалий, трудомісткий процес. Служба безпеки України, як одна з національних безпекових структур, активно займається питаннями впровадження стандартів НАТО у свою діяльність. Зокрема, створено робочу групу з євроатлантичної інтеграції, в рамках якої проводяться засідання з питань опрацювання стандартів та керівних документів НАТО, визначення спроможностей СБ України тощо. Робочою групою здійснено аналіз 81-го документу, відібрано та опрацьовуються 33 адміністративні стандарти та 3 керівні документи у сфері навчання, кадрового та медичного забезпечення, логістики, спеціального зв'язку, аналітичної роботи, а також кіберзахисту. Протягом останнього року завдяки спільній плідній праці окремих підрозділів СБУ видано чотири накази ЦУ СБУ, в яких враховані окремі положення відповідних стандартів НАТО. Іншими підрозділами Служби також здійснюються відповідні заходи впровадження сертифікації НАТО в їх діяльність.

Список використаних джерел

1. Пріоритети для партнерів: особливий формат співпраці з Альянсом допомагає зміцнювати обороноздатність URL: https://ukrainetonato.com.ua/standarty-nato/priorytety-dlya-partneriv-osoblyvyy-format-spivpratsi-z-aliansom-dopomahaie-zmitsniuvaty-oboronozdatnist/ (дата звернення 17.04.2024)

2. Шановні панове! URL: https://ippi.org.ua/sites/default/ files/rozvitokzakonodavstva_ ukrayini_u_sferi_oboroni_maket.pdf (дата звернення 25.032024)

3. Кривенко О. Проблеми розвитку системи військового законодавства та його адаптації до стандартів організації північноатлантичного договору (НАТО). *Розвиток законодавства України у сфері оборони: проблеми адаптації до стандартів НАТО та шляхи їх вирішення:* матеріали Наук.– практ. конф., 23 квіт. 2021 р. Київ: ПП Фенікс, 2021. С. 31–35.

4. Плешко Е. Військова стандартизація – єдина мова та важлива умова взаємосумісності в НАТО. Розвиток законодавства України у сфері оборони: проблеми адаптації до стандартів НАТО та шляхи їх вирішення: матеріали Наук.– практ. конф., 23 квіт. 2021 р. Київ: ПП Фенікс, 2021. С. 68–73.

5. Голопатюк Л.С., Литовченко В.М. Стандарти Альянсу. *Оборонний вісник*. 2016. № 12. С. 4–9.

6. Возняк С.М., Иващенко А.М., Пенковский В.И. Политика стандартизации Североатлантического Альянса. *Збірник наукових праць центру воєнно-стратегічних досліджень Національного університету оборони України*. 2016. № 2(57). С. 74–79.

7. Альона Гетьманчук, Маріанна Фахурдінова. Дискусійна записка, видана за підтримки Чорноморського трасту регіональної співпраці – проєкту Фонду Маршалла (США). Центр «Нова Європа».2019. URL: neweurope.org.ua/ wp-content/uploads/219/07/DP_Stand_NATO ukr inet.pdf.(дата звернення 14.04.2024).

8. Стандарти НАТО механізм і темпи впровадження, адаптація до українських реалій // Сайт МО України. URL: https://www.mil.gov. ua/news/ 2021/02/12/standarti-nato-mehanizm-i-tempi-vprovadzhennya-adaptacziyado-ukrainskih-realij/ (дата звернення 23.03.2024).

ДО ПИТАННЯ ВІДМЕЖУВАННЯ ПОСОБНИЦТВА ДЕРЖАВІ-АГРЕСОРУ ВІД СУМІЖНИХ ДІЯНЬ

Оксана КНИЖЕНКО
доктор юридичних наук, професор
співробітник СБУ

Наразі одним із найскладніших питань у правозастосовній діяльності є питання відмежування пособництва державі-агресору від суміжних діянь. Передусім, йдеться про відмежування від колаборaційної діяльності.

Варто зазначити, що у науковій літературі цьому питанню увага була приділена ще починаючи з 2022 року. Вчені надавали різноманітні поради з цього приводу. Однак, як засвідчують дані, що містяться у Єдиному державному реєстрі судових рішень (далі – Реєстр), суди не поспішали кваліфікувати дії осіб саме за ст. 111–2 КК України. Цьому, безумовно, спонукав сам текст закону про кримінальну відповідальність.

Так, пособництво державі-агресору за багатьма ознаками подібне до колаборaційної діяльності, оскільки в обох складах кримінальних правопорушень йдеться про допомогу державі-агресору, збройним формуванням та/або окупаційній адміністрації держави-агресора, яка надається в тій чи іншій формі.

Судова практика щодо застосування ст. 111–2 КК України є в сотні разів меншою, ніж за ст. 111–1 КК України. Така тенденція є сталою й характерна не тільки для 2023 року, але й станом на 21 червня 2024 року. Звертає на себе увагу й той факт, що вироки, які стосуються ст. 111–2 КК України, в згаданому Реєстрі почали опубліковуватися з травня 2023 року, на відміну від тих, що стосуються ст. 111–1 КК України, оскільки останні почали опубліковуватися в Реєстрі роком раніше, з квітня 2022 року. Таке обережне ставлення судів до ст. 111–2 КК України обумовлене законодавчою вадою, яка має місце. Зокрема, обидві норми не відповідають принципу правової визначеності. Відповідно до практики Європейського суду з прав людини у разі порушення принципу правової визначеності всі сумніви мають тлумачитися на користь винної особи.

Не претендуючи на безапеляційність запропонованих тверджень, висловлю низку положень, які були б орієнтиром відмежування проявів колаборaційної діяльності від пособництва державі-агресору.

Законодавець формулює для всіх форм пособництва державі-агресору спільні ознаки – це умисність дій, спрямованих на допомогу державі-агресору, збройним формуванням та/або окупаційній адміністрації держави-агресора, з метою завдання шкоди Україні. У такому загальному значенні пособництво державі-агресору схоже до колаборaційної діяльності, яка також вчиняється на шкоду Україні. Про завдання шкоди Україні безпосередньо не вказується у ст. 111–1 КК України, однак зважаючи на її місце розташування, а саме,– І Розділ Особливої частини КК України, шкода Україні завдається завжди, оскільки йдеться про основи національної безпеки України, що є об'єктом згаданих складів кримінальних правопорушень. Тому, зважаючи на положення ст. 2 КК України, де відзначається, що підставою кримінальної відпо-

відальності є вчинення особою суспільно небезпечного діяння, яке містить склад кримінального правопорушення, передбаченого КК України, державі Україна спричиняється шкода в обох кримінальних правопорушеннях.

Шкода про яку йдеться є ознакою не об'єктивної сторони складу кримінального правопорушення, а конститутивною ознакою об'єкта. Це означає, що під час доведення вини особи має враховуватися суб'єктивне ставлення особи до вчинюваного діяння, тобто усвідомлення того, що вчинюване нею діяння шкодить інтересам України й саме цього прагне винна особа. На наявність вказаної ознаки зазначається у вироках, що містяться в Реєстрі.

Передбаченість більш суворої санкції за допомогу державі-агресору про яку йдеться у ст. 111–2 КК України свідчить про підвищений рівень суспільної небезпечності діянь, описаних цією нормою. Це вочевидь обумовлено характером діянь, описаних ст. 111–2 КК України, а саме: реалізацією чи підтримкою рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора; добровільним збором, підготовкою та/або передачею матеріальних ресурсів чи інших активів представникам держави-агресора, її збройним формуванням та/або окупаційній адміністрації держави-агресора.

Реалізація чи підтримка рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора може проявлятися в різних формах. До них може належати й обіймання певних посад, завдяки яким втілюються у життя задуми держави-агресора. В такому контексті основним критерієм відмежування колабораційної діяльності від пособництва державі-агресору слугуватиме обізнаність про майбутні плани держави агресора, а не тільки підтримка та реалізація рішень окупаційної адміністрації. У такому разі підвищений рівень суспільної небезпечності діянь обумовлений масштабністю вчинюваних дій, їхнім значенням для політико-економічних напрямів України. Такий висновок підтверджується й матеріалами судової практики згідно з якими посади вищої ланки керівного складу розглядаються саме як пособництво державі-агресору, а не колабораційна діяльність (справа № 337/414/23 вирок Хортицького районного суду міста Запоріжжя від 30 травня 2023 року [1]; справа № 331/1897/23 вирок Жовтневого районного суду м. Запоріжжя від 02 серпня 2023 року [2], справа 953/6896/22 вирок Київського районного суду м. Харкова від 07 червня 2023 року [3], справа № 522/16244/22 вирок Приморського районного суду м. Одеси від 15 червня 2023 року [4]).

Пособництво державі-агресору подібне до колабораційної діяльності, що здійснюється у таких формах як передача матеріальних ресурсів незаконним збройним чи воєнізованим формуванням, створеним на тимчасово окупованій території, та/або збройним чи воєнізованим формуванням держави-агресора, та/або провадження господарської діяльності у взаємодії з державою-агресором, незаконними органами влади, створеними на тимчасово окупованій території, оскільки у ст. 111–2 КК України йдеться про добровільний збір, підготовку та/або передачу матеріальних ресурсів чи інших активів представникам держави-агресора, її збройним формуванням та/або окупаційній адміністрації держави-агресора.

Критеріями відмежування вказаних видів слугуватиме спрямованість дій та їхній характер. По-перше, у ст. 111–2 КК України йдеться не тільки про передачу матеріальних ресурсів, а й про їхній збір та підготовку. Ця норма передбачає значно ширше коло суб'єктів, яким можуть передаватися такі ресурси. Зокрема, ними будуть не тільки збройні формування держави-агресора, а й окупаційній адміністрації держави-агресора. Окрім ресурсів також можуть передаватися й активи.

Основним критерієм, який би дозволив відмежувати передачу матеріальних ресурсів незаконним збройним формуванням, про яку йдеться в обох нормах, від колабораційної діяльності, слугуватиме масштабність діяння, тобто його здатність впливати на об'єкт кримінального правопорушення. Приміром, якщо передача матеріальних ресурсів полягала у залученні широкого кола осіб (приміром, соціальних мереж), або значущості цих ресурсів для безпеки України. Подібна позиція узгоджується і з наявними матеріалами судової практики (вирок у справі № 496/350/23 від 25 травня 2023 року) [5].

З огляду на зазначене, дії суб'єктів господарювання, що спрямовані на передачу матеріальних ресурсів представникам держави-агресора, її збройним формуванням та/або окупаційній адміністрації держави-агресора, належить кваліфікувати за ст. 111–2 КК України, якщо до такої передачі залучалося широке коло осіб, або ці матеріальні ресурси мають стратегічне значення для України.

Тенденцією правозастосовної діяльності в 2024 році є поширювальне тлумачення положень ст. 111–2 КК України. Наприклад, як це має місце у вироці по справі № 127/9179/23 від 17 квітня 2024 року [6], яким особу було засуджено за співпрацю із представником міністерства оборони рф під час передавання відомостей щодо розташування Збройних сил України. Також судова практика пішла шляхом кваліфікації дій за сукупністю кримінальних правопорушень у разі обіймання посад, про які йдеться в ст. 111–1 КК України та реалізації рішень, описаних ст. 111–2 КК України (наприклад, вирок по справі № 521/13772/23 від 26 квітня 2024 року) [7].

Таким чином, через неоднозначність норм, описаних ст.ст. 111–1 та 111–2 КК України, наявна судова практика з розгляду вказаної категорії кримінальних проваджень є розрізненою. Це стоїть на заваді реалізації принципу справедливості, який є основою для судової системи будь-якої держави світу.

Усунути наявні недоліки можливо або шляхом формування Великою Палатою Верховного Суду правових висновків по даній категорії кримінальних проваджень, або шляхом внесенням змін до КК України.

Список використаних джерел:

1. Вирок у справі № 337/414/23 від 30 травня 2023 року. URL: https://reyestr.court.gov.ua/Review/111172842 (дата звернення 21.06.2024).
2. Вирок у справі №№ 331/1897/23 від 02 серпня 2023 року. URL: https://reyestr.court.gov.ua/Review/112562491 (дата звернення 21.06.2024).
3. Вирок у справі № 953/6896/22 від 07 червня 2023 року. https://reyestr.court.gov.ua/Review/111429509 (дата звернення 21.06.2024).
4. Вирок у справі № 522/16244/22 від 15 червня 2023 року. URL: https://reyestr.court.gov.ua/Review/111572074 (дата звернення 21.06.2024).
5. Вирок у справі № 496/350/23 від 25 травня 2023 року. URL: https://reyestr.court.gov.ua/Review/111089967 (дата звернення 21.06.2024).
6. Вирок у справі № 127/9179/23 від 17 квітня 2024 року. URL: https://reyestr.court.gov.ua/Review/118447852 (дата звернення 21.06.2024).
7. Вирок у справі № 521/13772/23 від 26 квітня 2024 року. URL:: https://reyestr.court.gov.ua/Review/118676189 (дата звернення 21.06.2024).

НАПРЯМИ МІЖНАРОДНОЇ ВЗАЄМОДІЇ УКРАЇНИ З ЄВРОПЕЙСЬКИМ СОЮЗОМ ЩОДО ЗАПОБІГАННЯ БЕЗПЕКОВИХ ЗАГРОЗ

Сергій КОНСТАНТІНОВ
доктор юридичних наук, професор,
співробітник СБУ

Сучасні форми політичної взаємодії між державами зазнали змін внаслідок нових вимог щодо забезпечення національної, європейської та міжнародної безпеки. Демократична політична взаємодія враховує різноманітні точки зору та напрями розвитку. Російсько-українська війна загострила важливість дотримання принципів функціонування та безпеки Європейсько-

го Союзу. Військова ескалація в Україні об'єднала суспільні інтереси країн ЄС та згуртувала їх населення. Сучасні безпекові виклики вказують на необхідність переформатування міжнародних інституцій для забезпечення стабільного розвитку суспільства.

Водночас вибір курсу України на вступ до ЄС вимагає адаптації національного законодавства до європейських стандартів у всіх сферах суспільного життя. Це стосується як забезпечення відповідності законів, ухвалених Верховною Радою України, зобов'язанням країни у сфері європейської інтеграції та праву Європейського Союзу (acquis ЄС), так і трансформації діяльності Кабінету Міністрів України. Останній є головним ініціатором відповідних законопроєктів, спрямованих на гармонізацію українського законодавства з правом acquis ЄС та виконання міжнародно-правових зобов'язань України в рамках європейської інтеграції [1].

З огляду на триваючу повномасштабну війну в Україні, дослідження правового регулювання безпекових відносин у країнах ЄС є вчасним та важливим. Дослідження умов та засад національної безпеки проводили такі вчені, як В.Б. Авер'янов, О.М. Бандурка, Ю.П. Битяк, Р.А. Калюжний, В.А. Ліпкан, В.Я. Настюк, Ю.В. Мех, О.С. Проневич та інші. Проте, враховуючи стратегічний курс України на повноправне членство в ЄС та необхідність розробки плану дій щодо забезпечення безпеки як всередині, так і поза межами ЄС у контексті російського вторгнення, питання впорядкування безпекових відносин в ЄС ще не розглядалося належним чином. Тому визначення поточного стану адміністративно-правового регулювання суспільних відносин у сфері безпеки на рівні ЄС та роль України у формуванні нової безпекової парадигми ЄС є надзвичайно актуальним питанням.

Загалом політика безпеки та оборони є невід'ємною складовою зовнішньої політики і політики безпеки ЄС. Формування єдиного підходу до вирішення безпекових питань у країнах-членах ЄС має на меті спільне врегулювання конфліктів та криз, захист громадян та зміцнення міжнародного правопорядку і безпеки [2]. Правовою основою для врегулювання питань безпеки стало прийняття Лісабонського договору. Цей договір запровадив європейську політику в сфері озброєння та його забезпечення, а також відкрив можливості для співпраці з іншими партнерами, такими як ООН, НАТО та Африканський союз [3].

Положення оновленого Договору про Європейський Союз у сфері безпеки та оборони охоплюють такі аспекти:

1. Спільна безпекова та оборонна політика є складовою спільної зовнішньої та безпекової політики ЄС, реалізованої за допомогою цивільних і військових засобів.

2. ЄС може застосовувати свої безпекові інструменти за межами Союзу для підтримання миру, запобігання конфліктам і зміцнення міжнародної безпеки.

3. Політика ЄС у сфері безпеки та оборони не повинна впливати на національну політику деяких держав-членів в рамках НАТО.

4. Держави-члени ЄС мають поступово підвищувати свій військовий потенціал відповідно до планів, визначених Агенцією з розвитку оборонного потенціалу, досліджень, закупівель та озброєння.

5. Рішення щодо спільної безпекової та оборонної політики приймаються одностайно на основі пропозиції Верховного представника Союзу з питань закордонних справ і політики безпеки або за ініціативою окремої держави-члена.

6. У разі збройної агресії проти держави-члена на її території, інші держави-члени зобов'язані допомогти всіма можливими засобами [4].

У протоколі № 10 до Договору про Європейський Союз «Щодо структурної співпраці, встановленої статтею 42 Договору про Європейський Союз» додатково визначено характеристики співпраці у сфері безпеки та оборони. Наприклад, акцент зроблено на підвищенні оборонного потенціалу через збільшення національних внесків, участь у багатонаціональних силах, основних європейських програмах оснащення та діяльності Агенції з розвитку оборонного потенціалу, досліджень, закупівель та озброєння [5]. У Деклараціях [6] та [7] щодо спільної зовнішньої та безпекової політики підкреслюється, що спільні заходи в рамках ЄС не повинні завдавати шкоди особливостям безпекової та оборонної політики держав-членів. Водночас,

спільна політика у сфері безпеки та оборони не впливає на правові засади, обов'язки та повноваження кожної держави-члена щодо формування та здійснення своєї зовнішньої політики, національної дипломатичної служби, відносин з третіми країнами та участі в міжнародних організаціях, включаючи членство в Раді Безпеки Організації Об'єднаних Націй.[5].

У 2016 році відбулося оновлення безпекової концепції в межах ЄС, що знайшло відображення в положеннях Глобальної стратегії ЄС у сфері зовнішньої політики та політики безпеки. Цей стратегічний документ, як приклад м'якого права, визначив пріоритети політики ЄС у сфері оборони, зокрема безпеку держав ЄС, стійкість держав і суспільства на сході та півдні ЄС, а також розробку комплексного підходу до конфліктів. У результаті було прийнято План реалізації в області безпеки та оборони. У цей період також було запропоновано створення Європейського Фонду оборони, який зосередився на питаннях оборонних досліджень і розвитку потенціалу. Серед програмних документів, що стосуються подальшого розвитку механізмів у сфері безпеки та оборони на рівні ЄС, варто виділити Аналітичний документ про майбутнє європейської оборони (2025 р.), прийнятий Європейською Радою в грудні 2016 року, який включає реалізацію Глобальної стратегії ЄС у сфері безпеки та оборони, План дій у сфері європейської оборони та співробітництво з НАТО. ЄС зобов'язаний захищати громадян і просувати європейські інтереси та цінності. Головна риса задекларованого підходу до вирішення безпекових питань полягає в поєднанні м'якої та жорсткої політики – інструменти безпеки та оборони використовуються разом із дипломатією, санкціями та співробітництвом. Хоча м'які регулятори можуть бути недостатніми, цей комплексний підхід лежить в основі концепту «стійкої безпеки» [8].

Лише у 2021 році було створено Стратегічний компас, де викладено стратегію безпеки та оборони. З огляду на ситуацію в Україні, цей документ було переглянуто, враховуючи внесок Комісії в європейську оборону та Версальську декларацію (10–11 березня 2022 року). Основна мета оновленої стратегії полягає в забезпеченні політичного керівництва для досягнення «стратегічної автономії» за такими напрямами: а) кризове управління; б) стійкість; в) можливості та партнерські відносини [9].

Повне розуміння ситуації у правовому регулюванні безпекових відносин у ЄС неможливе без урахування конкретних рішень, які приймаються уповноваженими інституціями Європейського Союзу у цій сфері. Наприклад, Європейський Парламент ухвалив ряд важливих резолюцій. Одна з таких резолюцій від 27 лютого 2014 року стосується використання військових дронів і встановлює включення цих збройних безпілотників до відповідних європейських та міжнародних режимів роззброєння і контролю за озброєнням. Вона також передбачає заборону на розробку, виробництво та використання повністю автономних засобів, які можуть завдавати ударів без участі людини. Інша важлива резолюція від 11 грудня 2018 року «Про військову мобільність» акцентує увагу на значущості сприяння міжсекторальній співпраці між державами-членами для розвитку двосторонньої мобільності. Це дозволяє оперативно реагувати на кризові ситуації шляхом швидкого та ефективного розгортання військових сил і ресурсів для місій і операцій, що гарантує статус ЄС як надійної інституції, яка забезпечує глобальну безпеку [11]); резолюцію від 17 вересня 2020 року «Про експорт озброєнь: реалізація загальної позиції» [10] тощо.

Значимість резолюції Європейського Парламенту від 7 липня 2021 року «Про співробітництво ЄС-НАТО у контексті трансатлантичних відносин» підкреслює необхідність подальшого зміцнення співпраці та партнерства між Європейським Союзом та НАТО для ефективного відповіді на виклики безпеки. Документ визнає мілітаристську політику Росії як загрозу для безпеки держав-членів ЄС та НАТО. Отже, важливим для обох організацій є розробка послідовної та активної стратегії відповіді на традиційні та гібридні акти агресії та провокацій з боку Росії. Це передбачає посилення протидії прямим і непрямим акціям Росії проти України, Грузії та Молдови, а також її активності в регіонах Балтійського і Чорного морів, у Азовському морі та Східному Середземномор'ї. Одним із ключових аспектів трансформації правового регулювання безпекових питань у ЄС є зміцнення взаємодії з міжнародними організаціями

та постійне удосконалення цього процесу для досягнення високого рівня безпеки, зберігаючи водночас автономію держав-членів ЄС у справах національної безпеки та участі в міжнародних місіях безпеки.

Деякі юридичні акти, які діють на території Європейського Союзу та стосуються сфери безпеки, були прийняті за участю Європейського парламенту та Ради ЄС. Наприклад, Регламент 2021/697 від 29 квітня 2021 року, що стосується створення Європейського оборонного фонду, є одним із таких актів. Також варто звернути увагу на рішення, які прийняла Рада ЄС, зокрема: рішення Ради (CFSP) 2017/2315 від 11 грудня 2017 року, яке регулює налагодження постійного структурованого співробітництва (PESCO) та визначає перелік держав-учасниць, і рішення Ради (CFSP) 2021/2315 від 22 березня 2021 року, що стосується створення Європейського фонду безпеки.

Отже, адаптація національного законодавства України у сфері безпеки та оборони до стандартів ЄС означає приведення законів та підзаконних нормативно-правових актів у відповідність до положень права ЄС. Ці положення включають акти, прийняті Європейським парламентом та Радою ЄС, а також акти Агенції у сфері розвитку оборонного потенціалу, досліджень, закупівель та озброєння, які деталізують такі аспекти, як:

а) зміцнення національної обороноздатності та самостійності у питаннях безпеки;

б) поглиблення співробітництва між державами-членами ЄС та взаємодія між ЄС та НАТО у сфері безпеки.

Закріплення в Стратегії зовнішньополітичної діяльності України курсу на набуття повноправного членства країни в ЄС та НАТО зумовлене рядом чинників, включаючи сприйняття ЄС як провідного глобального актора у сфері захисту прав людини. НАТО в той же час розглядається як основний суб'єкт забезпечення безпеки на євроатлантичному просторі, не зважаючи на тенденції до зміцнення стратегічної автономії ЄС у сфері безпеки та оборони [12].

На рівні ЄС виділяються три підходи до подальшої трансформації політики безпеки й оборони, які варто ураховувати українській державі:

Перший підхід полягає в активній співпраці у сфері безпеки й оборони. Ця стратегія включає в себе виконання місій для підвищення обороноздатності, проведення невеликих операцій для урегулювання криз, інтенсивний обмін розвідданими, а також підтримку стійкості держав-членів ЄС і співпрацю з ЄС-НАТО. Однак недоліком є обмежена можливість розробки ключових оборонних технологій на рівні ЄС та обмежене використання європейських оборонних ресурсів.

Другий підхід спрямований на формування загальної безпеки та захисту. Реалізація цієї концепції можлива через поліпшення антикризового управління, нарощування потенціалу і захист внутрішніх і зовнішніх зв'язків, контроль і допомогу в кіберпросторі, обмін інформацією та координацію дій ЄС-НАТО в усіх аспектах безпеки. Цей підхід передбачає спільне фінансування національних оборонних програм за підтримки Європейського оборонного фонду.

Третій підхід спрямований на формування загального захисту та безпеки. Цей варіант передбачає проведення спільного моніторингу та оцінки загроз, планування в разі непередбачених обставин, а також забезпечення кібербезпеки на рівні ЄС. Європейська система спільної безпеки та оборони, доповнюючи НАТО, сприяє підвищенню стійкості Європи та захисту від різних форм агресії проти ЄС [13].

Узагальнюючи, можна зазначити, що війна в Україні спричинила потребу перегляду всієї існуючої безпекової концепції ЄС. Виникаючі загрози стосуються як національної безпеки держав-членів ЄС, так і глобальної безпеки. В умовах сучасності політика безпеки ЄС повинна бути переглянута з метою максимального задіяння колективного оборонного потенціалу, зберігаючи при цьому національну автономію у вирішенні окремих питань. Особливо важливим у формуванні нового підходу до забезпечення світової безпеки є зміцнення взаємодії між ЄС та НАТО. Для України ці тенденції визначають напрямок під час реформування національного законодавства у сфері безпеки й оборони та його адаптації до стандартів ЄС.

Список використаних джерел:

1. Про деякі заходи щодо виконання зобов'язань України у сфері європейської інтеграції: Постанова Верховної Ради України від 29.07.2022 р. № 2483-IX. URL: https://zakon.rada.gov.ua/laws/show/2483–20#Text. (дата звернення: 18.06.2024)
2. Common security and defence policy. URL: https://www.europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy. (дата звернення: 18.06.2024)
3. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT. (дата звернення: 18.06.2024)
4. Консолідована версія Договору про Європейський Союз. Офіційний вісник Європейского Союзу. 2010. URL: https://zakon.rada.gov.ua/laws/show/994_b06#Text. (дата звернення: 18.06.2024)
5. Консолідовані версії договору про Європейський Союз (вчиненого в Маастрихті сьомого дня лютого тисяча дев'ятсот дев'яносто другого року) та договору про функціонування Європейського Союзу (вчиненого в Римі двадцять п'ятого дня березня місяця року одна тисяча дев'ятсот п'ятдесят сьомого). URL: https://zakon.rada.gov.ua/laws/show/994_b06#Text. (дата звернення: 18.06.2024)
6. Декларація 13 щодо спільної зовнішньої та безпекової політики. Офіційний вісник Європейского Союзу. 2010. URL: https://zakon.rada.gov.ua/laws/show/994_b06#Text. (дата звернення: 18.06.2024)
7. Декларація 14 щодо спільної зовнішньої та безпекової політики. Офіційний вісник Європейского Союзу. 2010. URL: https://zakon.rada.gov.ua/laws/show/994_b06#Text. (дата звернення: 18.06.2024)
8. Commission communication of 7 June 2017 entitled 'Reflection Paper on the Future of European Defence. Reflection paper on the feture of Europian defence. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0315. (дата звернення: 18.06.2024)
9. Common security and defence policy. URL: https://www.europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy. (дата звернення: 18.06.2024)
10. European Parliament resolution of 17 September 2020 on Arms export: implementation of Common Position 2008/944/CFSP (2020/2003(INI)). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020IP0224. (дата звернення: 18.06.2024)
11. European Parliament resolution of 7 July 2021 on EU-NATO cooperation in the context of transatlantic relations. URL: https://www.europarl.europa.eu/doceo/document/TA-9–2021–0346_EN.html. (дата звернення: 18.06.2024)
12. Про рішення Ради національної безпеки і оборони України від 30 липня 2021 року «Про Стратегію зовнішньополітичної діяльності України»: Указ Президента України від 26.08.2021 р. № 448/2021. URL: https://zakon.rada.gov.ua/laws/show/448/2021#n11. (дата звернення: 18.06.2024)
13. Мартинов А. Спільна зовнішня і безпекова політика Європейського Союзу: основні етапи розвитку. Європейські історичні студії. 2015. № 1. С. 43–61.

КОНКУРЕНЦІЯ КРИМІНАЛЬНО-ПРАВОВИХ НОРМ ПРИ КВАЛІФІКАЦІЇ ДИВЕРСІЇ

Олександр ЛАЗАРЕНКО
співробітник СБУ

Законодавча еволюція кримінально-правової норми, якою передбачена кримінальна відповідальність за диверсію, в частині визначення її форм суспільно небезпечного діяння, свідчить, що впродовж свого існування вона зазнавала істотних змін. Так, на початку свого існування диверсія полягала лише у знищенні чи пошкодженні тих чи інших важливих предметів.

За КК 1960 року норма була доповнена такими формами вчинення злочину як вчинення масових отруєнь або поширення епідемій та епізоотій. Згодом до вказаних форм вчинення диверсії додалися форми вчинення дій, спрямовані на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їх здоров'ю.

У 1992 році ст. 60 КК була доповнена формою вчинення дій, спрямованих на поширення епіфітотій.

За чинним КК усі вищевказані форми диверсії знайшли своє відображення у ст. 113 КК. Крім того, в диспозиції цієї статті у 2001 році з'явилась нова форма злочину, що полягає у вчиненні дій, спрямованих на радіоактивне забруднення. Так, статтею 113 КК України передбачена кримінальна відповідальність за вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій [1, с. 126].

До того ж відбулась і трансформація покарання за вчинення диверсії. Так, якщо ст. 60 КК України (1960) в редакції станом на 2000 рік передбачала покарання у вигляді позбавлення волі на строк від десяти до п'ятнадцяти років з конфіскацією майна або довічне позбавлення волі з конфіскацією майна то вже у КК України (2001) довічне позбавлення волі було виключено із можливих видів покарання за цей злочин.

Чинна юридична конструкція ст. 113 КК України сформульована за принципом усіченого складу злочину, момент закінчення якого перенесено законодавцем на стадію замаху на його вчинення. Для формування конструкції складу злочину проти основ національної безпеки це є притаманним способом, адже таким чином сформульовані майже всі кримінально-правові норми, що розташовані у розділі І Особливої частини КК України. Основним призначенням таких конструкцій є підсилення кримінальної відповідальність винної особи за злочини із підвищеною суспільною небезпечністю. Проте застосування такої конструкції у диспозиції ст. 113 КК України, а також кримінально-правових санкцій щодо цього злочину порушило принцип системності її формування.

Зокрема це простежується при застосуванні порівняльного аналізу даного злочину із суміжними складами кримінальних правопорушень та іншими злочинами проти основ національної безпеки. Так ст. 112 КК України, якою визначено підстави кримінальної відповідальності за посягання на життя державного чи громадського діяча передбачено покарання позбавлення волі на строк від десяти до п'ятнадцяти років або довічне позбавленням волі з конфіскацією майна або без такої. Навіть з урахуванням того, що даний вид кримінального правопорушення сформовано законодавцем з урахуванням конструкції усіченого складу злочину, момент закінчення якого перенесено на стадію замаху.

Окремі недоліки законодавчої конструкції ст. 113 КК України проглядаються у порівняні із визначенням об'єктивної сторони злочину передбаченого ст. 258 КК України. Зокрема, застосування зброї, вчинення вибуху, підпалу чи інших дій, якщо вони призвели до загибелі людини караються позбавленням волі на строк від десяти до п'ятнадцяти років або довічним позбавленням волі з конфіскацією майна або без такої. Натомість ст. 113 КК України не передбачає такої кваліфікуючої ознаки як загибель людини. До того ж санкція цієї кримінально-правової норми не має і такого виду покарання як довічне позбавлення волі.

Таким чином сформульована законодавцем диспозиція ст. 113 КК України представляє собою складену кримінально-правову норму і у разі настання тяжких наслідків у вигляді загибелі людини з'являється кримінально-правова конкуренція частини і цілого. В юридичній літературі даний вид є конкуренцією кримінально-правових норм, за якого вчинений злочин підпадає під дію двох (або більшої кількості) кримінально-правових норм, одна з яких – ціле, охоплює вчинене в цілому та разом, а друга (інші) – норми-частини, які визнають як самостійні злочини лише частини вчиненого суспільно небезпечного посягання [2].

Правила кваліфікації при конкуренції частини і цілого у юридичній літературі визначені наступним чином: якщо ознаки складу злочину, передбаченого нормою частиною, повністю охоплюються ознаками складу злочину, передбаченого нормою-цілим, а санкція статті (частини статті) Особливої частини КК, що передбачає норму-ціле, є більш суворою, ніж санкція статті (частини статті) Особливої частини КК, що передбачає норму-частину, кваліфікація за сукупністю злочинів виключається [3, с.147].

Натомість в контексті кваліфікації суспільно небезпечного діяння, передбаченого ст. 113 КК України у разі настання суспільно небезпечних наслідків у вигляді загибелі людей ми маємо ситуацію, коли частина за своєю санкцією значно перевищує ціле, адже відповідно до диспозиції ч. 2 ст. 115 КК України умисне вбивство карається позбавленням волі на строк від десяти до п'ятнадцяти років або довічним позбавленням волі, з конфіскацією майна у випадку, передбаченому пунктом 6 частини другої цієї статті.

Таким чином подібні кримінально-правові ситуації мають кваліфікуватись за правилами ідеальної сукупності – ст. 113 та ч. 2 ст. 115 КК України.

Список використаних джерел:

1. Климосюк А. Законодавча конструкція диверсії: реалії та перспективи. Національний юридичний журнал: теорія та практика. Квітень 2018. С. 125–128

2. Марін О.К. Кваліфікація злочинів при конкуренції кримінально-правових норм. К.: Атіка, 2004. 224 с.

3. Теорія та практика кримінально-правової кваліфікації: лекції. Харків: Право, 2018.– 368 с.: іл.

СУЧАСНІ РЕАЛІЇ ДОКУМЕНТУВАННЯ ТА ДОСУДОВОГО РОЗСЛІДУВАННЯ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ НА ДЕОКУПОВАНИХ ТЕРИТОРІЯХ УКРАЇНИ

Леонід МЕДВЕДЮК
співробітник СБУ

Станом на лютий 2022 року російською федерацією було окуповано 43 300 км2, або 7% території України, а саме АР Крим та місто Севастополь, частини Донецької та Луганської областей. У квітні 2014 року та у березні 2015 року Верховна Рада України визначила статус цих території, як тимчасово окуповані території України.

Після 24 лютого 2022 року у результаті повномасштабного вторгнення площа таких територій зросла, країною-агресором – Російською Федерацією було додатково окуповано окремі території районів Донецької, Житомирської, Запорізької, Луганської, Миколаївської, Сумської, Чернігівської, Харківської та Херсонської областей.

Частина з цих територій і по теперішній час перебувають під окупацією країни-агресора. Частину ж окупованих Російською Федерацією територій України вдалося звільнити від загарбника і вони потребують відновлення на них нормальної життєдіяльності громадян України, відновлення української влади, що включає в себе забезпечення правопорядку та безпеки. Тому, така робота на деокупованих територіях України надзвичайно актуальна та важлива як для держави України так і для українського суспільства в цілому.

Органами та підрозділами Служби безпеки України на деокупованій території України проводяться заходи із виявлення, документування та розслідування:

– фактів загибелі цивільного населення України у результаті збройної агресії РФ;

– фактів порушень законів та звичаїв війни представниками Російської Федерації;
– фактів обстрілів і руйнувань цивільної та критичної інфраструктури України;
– диверсійної діяльності;
– розвідувально-підривної діяльності;
– колабораційної діяльності.

З метою протидії диверсійній та розвідувально-підривній діяльності РФ органами і підрозділами СБ України проводяться відповідні антидиверсійні та контррозвідувальні заходи (виявлення та знешкодження диверсійно-розвідувальних груп, їх сил та засобів, затримання державних зрадників та колаборантів, документування і припинення їх діяльності), процесуальні заходи з документування такої протиправної діяльності та притягнення у рамках досудового розслідування винних осіб до кримінальної відповідальності за вчинення вищезгаданих злочинів.

Окреме місце в заходах, які проводяться СБ України, як на окупованій території, так і на деокуповній території України, займає документування, протидія та припинення колабораційної діяльності громадян України.

Колабораційна діяльність є допомогою ворогу у посяганні на основу основ держави – її суверенітет, територіальну цілісність та недоторканність, обороноздатність, державну, економічну та інформаційну безпеку України.

Тому, організація Службою безпеки України виявлення, документування і розслідування злочинів колаборантів на де окупованих територіях має особливе значення.

Досудове розслідування у кримінальних провадженнях про колабораційну діяльність має свої особливості, зокрема, як правило розслідування розпочинається:

– за матеріалами та повідомленням оперативних підрозділів СБУ (за результатами ведення ними оперативно-розшукових та контррозвідувальних справ, матеріалами перевірки заяв та звернень громадян, повідомлень у засобах масової інформації та на підставі перевірок відомостей про колабораційну діяльність у мережі Інтернет);
– за заявами та зверненнями громадян;
– за повідомленнями ЗМІ;
– як самостійне виявлення слідчим або прокурором ознак кримінального правопорушення у ході розслідування інших злочинів.

У таких кримінальних провадженнях здійснюються першочергові слідчі дії та заходи:

– огляди джерел, які містять фактичні дані про вчинення правопорушення (фото, відеоматеріалів, інформації з мережі Інтернет, телефонів, ПЕОМ, документів, тощо);
– огляди місця події (місця розташування органів окупаційної влади, місць проведення псевдореферендумів);
– обшуки за місцями проживання осіб, які обґрунтовано підозрюються у колабораційній діяльності;
– допити свідків, потерпілих, спеціалістів;
– впізнання за фото, відеоматеріалами;
– проведення комплексу негласних слідчих дій стосовно колаборантів та їх російських кураторів;
– призначення експертиз (фото, відео, почеркознавчих, комп'ютерних, лінгвістичних, психіатричних, психологічних та інших);
– тимчасові доступи та витребування відомостей, що мають значення у справі (відомостей про мобільні з'єднання та місцеперебування абонентів у операторів мобільного зв'язку).

Практики відмічають наявність таких основних складнощів та проблем, що виникають під час досудового розслідування колабораційної діяльності:

– великий обсяг роботи по документуванню (вирішується шляхом відрядження на де окуповані території України слідчих та оперативних співробітників з інших регіонів України, створення з їх числа оперативно-слідчих міжвідомчих груп, грамотна розстановка сил і засобів, детальне планування роботи);

– небажання місцевого населення свідчити проти своїх земляків, через зневіру та страхи, що зс рф повернуться, через ментальну рису, що називають «моя хата скраю…» (відповідну роз'яснювальну роботу у цьому напрямку ведуть українські ЗМІ, місцеві активісти, волонтери, органи військово-цивільних адміністрацій);
– небажання місцевого населення свідчити проти своїх земляків, через страхи помсти від місцевих дрібних колаборантів (вирішується шляхом оприлюднення вироків судів про засудження таких осіб за колабораційну діяльність, розповсюдження матеріалів у соціальних мережах, групах в різних месенджерах; використання як заходу забезпечення безпеки свідка зміни їх анкетних даних особи, яка дає викривальні свідчення, показове затримання колаборантів і висвітлення такої роботи в ЗМІ та соціальних мережах);
– необхідність виділення серед маси колаборантів, у першу чергу тих осіб, діяльність яких має значний суспільний резонанс;
– більшість колаборантів, які залишились на деокупованих територіях та легко йдуть на угоду зі слідством, як і раніше йшли на співпрацю з окупантом, отримують вироки, де встановлено покарання не пов'язане з реальним позбавленням волі. Схильність таких осіб легко йти на угоду із досудовим слідством (прокурором) полегшує роботу слідства, однак не завжди схвально сприймається місцевим населенням (як пропозиція, вважалось би за доцільне включити до санкції усіх частин ст. 111–1 КК України[1] такий вид додаткового покарання, як конфіскація майна; штраф у частини 1 і 2 даної статті. А також, було б доцільним внести зміни до КК України, які б дали змогу судам у кримінальних провадження про колабораційну діяльність, у разі застосування положень ст. 75 КК України про звільнення особи від відбування покарання з випробовувальним строком, замінити таке покарання штрафом. Що, на думку практиків, було б більш дієво і позитивно впливало б на оперативну обстановку);
– відсутність узагальненої судової практики у справах про колабораційну діяльність. Юридична недосконаліть конструкції диспозиції ст. 111–1 КК України [1] та її схожість з злочинами, передбаченими ст. 111, 436–2, 260 КК України призводить до складності у правильній кваліфікації дій колаборантів, до неправильного застосування такої норми матеріального права, як на стадії досудового розслідування так і судового розгляду. (потрібно, щоб Верховний Суд України узагальнив судову практику у таких кримінальних провадженнях і прийняв відповідне рішення. Також необхідний комплексний підхід до цієї проблеми – законодавча діяльність та судове тлумачення чинної норми права у рішеннях ВСУ)

Таким чином складності та проблеми, які виникають під час організації виявлення, документування та досудового розслідування злочинів колаборантів вже вирішуються на практиці та можуть бути усунуті або подолані у подальшому через вжиття вищевказаних заходів.

Список використаних джерел:

1. Кримінальний кодекс України від 5 квітня 2001 року, № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text (дата звернення 01.06.2024).

АКТУАЛЬНІ ПРОБЛЕМИ РОЗСЛІДУВАННЯ СБ УКРАЇНИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ МИРУ, БЕЗПЕКИ ЛЮДСТВА ТА МІЖНАРОДНОГО ПРАВОПОРЯДКУ

Геннадій МЕЛЬНИК
співробітник СБУ

Міжнародне гуманітарне право є частиною міжнародного права, і застосовується тоді, коли відбувається збройний конфлікт. Розпочата повномасштабна збройна агресія росії проти України є грубим порушенням міжнародного права. Після початку російського вторгнення було проголошено Декларацію про створення Спеціального трибуналу для покарання злочину агресії проти України подібно до Лондонської декларації 1942 року, яка свого часу заклала основу для Нюрнберзького трибуналу. На сьогодні за статистичними даними Офісу Генерального прокурора станом червень 2024 року зареєстровано більше 134 тисяч кримінальних проваджень за фактами вчинення кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку, них майже 130 тисяч стосуються статті 438 Кримінального кодексу України «Порушення законів та звичаїв війни» [1].

Водночас, за результатами аналізу статистики судових вироків у Єдиному державному реєстрі судових рішень щодо міжнародних злочинів у період з 2014 по 2023 рік можна вивести орієнтовну цифру винесених обвинувальних вироків в Україні: 26 вироків за статтею 436 КК України «Пропаганда війни»; 514 вироків за статтею 436–2 КК України «Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників»; 11 вироків за статтею 437 КК України «Планування, підготовка, розв'язування та ведення агресивної війни», один з яких є виправдувальним; 31 вирок за статтею 438 КК України «Порушення законів та звичаїв війни»; відсутні вироки за статтею 441 КК України «Екоцид»; 3 вироки за статтею 442 КК України «Геноцид» тощо. Таким чином, загальними національними судами України за вищезазначеними злочинами винесено орієнтовно всього 585 вироків [2,3].

На органи СБ України (які згідно статті 216 КПК України розслідують кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку) покладається важливий обов'язок із належного збору, аналізу, збереження і зберігання доказів, забезпечення повноти з'ясування фактів та встановлення винних осіб, що вчинили відповідне кримінальне правопорушення передбачене главою XX Кримінального кодексу України.

Слід зазначити, що питому вагу у зборі таких доказів відіграє контррозвідувальна діяльність СБ України. Міжнародні стандарти розслідування вказують, що ретельність проведення і належне оформлення контррозвідувальних заходів є одним з найголовніших критеріїв успіху ефективності розслідування такої категорії кримінальних правопорушень та використання результатів контррозвідувальної діяльності як доказів у суді [4].

З іншої сторони, на сьогодні практична діяльність оперативних та слідчих підрозділів СБ України стикається з низкою правових та практичних проблем у розслідуванні кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку.

Перш за все, вбачається невідповідність вітчизняного кримінального законодавства загальновизнаним положенням міжнародного кримінального права, закріпленим у Римському статуті Міжнародного кримінального суду (бланкетна диспозиція статті 438 КК України, загальний суб'єкт злочину агресії, відсутність відповідальності за злочини проти людяності, відсутність інституту командної відповідальності тощо). Оскільки під час розслідування воєнних злочинів рф виникає необхідність взаємодії правоохоронних органів України з відповідними органами іноземних держав (Німеччини, Польщі, Франції тощо) то і нормативна база співпраці має бути,

на нашу думку, теж уніфікована. По-друге, вітчизняне законодавство має нормативні прогалини в частині правового механізму реалізації контррозвідувальних матеріалів у кримінальному процесі на відміну від оперативно-розшукових матеріалів. Це призводить до судових прецедентів неврахування матеріалів контррозвідувальних підрозділів СБ України як доказів.

По-третє, мають місце і проблеми організаційно-тактичного рівня в роботі слідчих та оперативних підрозділів СБ України. Часто це може проявлятись у неможливості: залучення до розслідування необхідних фахівців або спеціального обладнання як для пошуку і фіксації слідів злочину, забезпечення безпеки пересування слідчих бригад, слідчо-оперативних груп у районах збройного конфлікту тощо.

По-четверте, під час допуску іноземних слідчих/прокурорів до процесу розслідування воєнних злочинів в Україні, а саме участі в слідчих та процесуальних діях, виникає реальна проблема в обміні інформацією, яка, серед іншого, містить таємницю досудового розслідування або зібрана під час контррозвідувальної діяльності органами СБ України та має гриф обмеження доступу.

По-п'яте, кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку відносяться до підслідності СБ України, однак, як показує практика, розслідують їх іноді підрозділи Національної поліції, при цьому виникають проблемні аспекти взаємодії у виконанні доручення слідчих та передачі інформації працівниками оперативних підрозділів СБ України в порядку ст. 40 КПК України.

Вищевикладене доводить, що Україна наразі потребує удосконалення національної системи переслідування за кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку: приведення у відповідність міжнародного і вітчизняного законодавства, врегулювання правового механізму використання результатів контррозвідувальної діяльності у кримінальному процесі, утворення і навчання спеціалізованих підрозділів із розслідування такого роду кримінальних правопорушень, налагодження взаємодії з вітчизняними та міжнародними правоохоронними органами, залучення додаткових матеріально-технічних ресурсів, запровадження міжнародних стандартів розслідування міжнародних злочинів у вітчизняну практику кримінального процесу, удосконалення методів збору доказової й іншої значущої (передусім, розвідувальної, контррозвідувальної, криміналістичної, організаційно-забезпечувальної та іншої інформації).

Більш того, вважаємо, що важливим аспектом підсилення ефективності розслідування СБ України кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку є більш активне залучення до розслідування саме оперативних підрозділів, які проводять контррозвідувальну діяльність; навчання оперативних працівників щодо застосування нових можливостей OSINT з використанням стандартів протоколу Берклі і акцентування уваги на те, що виконуючи доручення слідчого вони мають ті ж повноваження, що і сам слідчий. Вищезазначене дає можливість значно оперативніше проводити досудове розслідування та зібрати докази у кримінальному провадженні щодо кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку та.

Список використаних джерел:

1. Єдиний реєстр судових рішень URL: https://reyestr.court.gov.ua (дата звернення 14.06.2024).

2. Офіс Генерального прокурора України URL: https://gp.gov.ua (дата звернення 14.06.2024).

3. Судові процеси щодо обвинувачення російських військових: чи діють гарантії ст. 6 ЄКПЛ? URL: https://www.helsinki.org. ua/articles/sudovi-protsesy-shchodo-obvynu vachennia-rosiyskykh-viyskovykh-chy-diiutharantii-st-6-yekpl(дата звернення 15.06.2024).

4. The Geneva Academy of International Humanitarian Law and Human Rights, ICRC, Guidelines On Investigating Violations Of International Humanitarian Law: Law, Policy, And Good Practice, 2019, § 137. URL: https://www.icrc.org/en/document/guidelines-investigating-violations-ihl-law-policy-and-good-practice (дата звернення 12.06.2024).

ПРОТИДІЇ ЗЛОЧИНАМ, ЩО ПОВ'ЯЗАНІ ІЗ ПРОТИПРАВНИМ ЗАВОЛОДІННЯМ МАЙНОМ ПІДПРИЄМСТВА, УСТАНОВИ, ОРГАНІЗАЦІЇ: ЗАРУБІЖНИЙ ДОСВІД

Кристіна МИРГОРОДСЬКА
аспірантка наукової лабораторії
з проблем протидії злочинності ННІ № 1
Національної академії внутрішніх справ

Сучасні процеси глобалізації, інтернаціоналізації та триваючої конвергенції потребують глибшого знання не тільки власного законодавства, а й законодавства, зокрема кримінального та кримінально-процесуального зарубіжних країн. Тим паче, що сьогодні Україна прагне стати повноправним членом Європейського Союзу і НАТО, а тому має привести своє законодавство у відповідність до європейських стандартів [1].

На сучасному етапі становлення України як європейської держави реалізується комплекс стратегічних заходів, спрямованих на розвиток економіки в умовах євроінтеграції [2]. Але, кризові явища в сучасній ринковій економіці зумовили нарощування в суспільстві криміногенного потенціалу. У цих умовах особливого значення набувають питання, пов'язані зі зміцненням системи національної безпеки, і, насамперед, безпеки економічної, орієнтованої на забезпечення стабільного розвитку суспільства і держави, їх захищеності від кримінальних загроз. Однією з таких порівняно нових для української кримінологічної дійсності загроз виступає феномен протиправного заволодіння майном підприємств, установ, організацій, так зване рейдерство. Це економічне за своєю суттю і кримінальне за формою і змістом явище в останні роки отримало досить широке поширення в Україні. Це, своєю чергою, дуже негативно впливає на економіку країни [3, с. 74].

Слід відзначити, що стосується реального стану й масштабів рейдерства, то варто зазначити, що інтегрованої офіційної статистики злочинів, пов'язаних із цим явищем, сьогодні не існує. Наявні офіційні дані щодо застосування ст. 206² Кримінального кодексу (далі – КК) України (протиправне заволодіння майном підприємства, установи, організації), на жаль, жодним чином не відображають дійсного поширення рейдерства [4, с. 138–139].

У зв'язку із тим, що рейдерство направлене на здійснення злочинних посягань на право власності та на економічний порядок, що безпосередньо загрожує економічній та національній безпеці України державна політика протидії злочинам, що пов'язані із протиправним заволодінням майном підприємства, установи, організації повинна бути спрямована на запровадження позитивного зарубіжного досвіду щодо визначення можливих шляхів їх вирішення (запобігання та протидії) з урахуванням сучасних умов в Україні.

Спеціальними нормативно-правовими актами, що регулюють недружнє поглинання, злиття, реорганізацію, реструктуризацію, викуп, що уособлюють в собі рейдерство (корпоративні відносини):

- США є закони: Шермана (the Sherman Antitrust Act) (1890), Клейтона (the Clayton Antitrust Act) (1914), Вільямса (the Williams Act) (1968) та Ріко (The Racketeer Influenced and Corrupt Organizations Act («RICO Act» або «RICO»)) (1970);
- –ЄС: Директива 2004/25/ЕС Європейського парламенту і Ради від 21 квітня 2004 року та Регламент (ЄС) 2019/452 Європейського парламенту і Ради від 19 березня 2019 р. з питань перевірки прямих іноземних інвестицій (ПІІ), який п застосовується в усіх державах-членах з 11 жовтня 2020 року;
- Великої Британії: Закон «Про конкуренцію» (The Competition Act) (1998), Закон «Про підприємницьку діяльність» (Enterprise Act) (2002), Акт про компанії (Companies Act)

(2006), що включає в себе такі документи: угода акціонерів (Shareholders Agreement); угода купівлі (продажу (Sale and Purchase Agreement), Закон про національну безпеку та інвестиції» (2022);

– Іспанія: Закон про королівський декрет (RDL) (Real Decreto-ley 8/2020) (2020);
– Італія: Закон «Golden Power» та законодавчий декрет № 23 від 2020 року «Невідкладні заходи щодо доступу до кредитів та дотримання податкового законодавства для компаній, спеціальні повноваження в стратегічних секторах, а також заходи щодо охорони здоров'я та роботи, продовження адміністративних та процесуальних строків судового розгляду). Окремо слід виокремити Глава I, розділ XIII «Злочини проти власності» Кримінальний кодекс Італії об'єднано відповідні заборони, які регулюють відповідальність за порушення прав на землю, особливо прав на нерухоме майно: ст. 631 – «Незаконне привласнення» (Usurpazione); ст. 633 – «Захоплення земель чи будівель» (Invasione di terreni o edifici); ст. 634 – «Насильницьке порушення володіння нерухомістю» (Turbativa violenta del possesso di cose immobili);
– Німеччина: Акціонерний Закон (1965), «Добровільний кодекс про ворожі поглинання» (1995), Постанови про зовнішню торгівлю і платежі (Außenwirtschaftsverordnung / AWV).(2021);
– Франції: Закон про торгові товариства (1966); Декрет про торгові товариства (1967); Ордонанс про свободу встановлення цін і про вільну конкуренцію. Торговий кодекс Французької Республіки містить норми кримінально-правового характеру, які захищають корпоративні відносини (1986). Указ № 2020–892 від 22 липня 2020 року щодо тимчасового зниження порогу контролю іноземних інвестицій у французьких компаніях, акції яких допущені до торгів на регульованому ринку. А також у розділі IV Торгівельного кодексу Франції (1807), врегульовано питання корпоративних конфліктів, що передбачає кримінальну відповідальність за правопорушення, пов'язані з діяльністю комерційних організацій та інших злочинів у сфері корпоративних відносин;
– Кримінальний кодекс Республіки Молдова передбачає дії, що охоплюються поняттям «рейдерство», зокрема: ст. 245–2 «Порушення законодавства при веденні реєстру власників цінних паперів/інвестиційних паїв», ст. 245–4 «Порушення положень про порядок укладення угод з майном комерційних товариств», ст. 245–5 «Умисна відмова у розкритті і/або представленні інформації, передбаченої законодавством, про небанківський або банківський фінансовий ринок», ст. 245–9 «Перешкоджання реалізації права учасників (акціонерів) комерційних товариств і незаконне позбавлення цих прав», ст. 246 «Обмеження вільної конкурентності», ст. 246–1 «Недобросовісна конкуренція», ст. 247 «Примушення до укладання угоди або відмови від її укладання», ст. 252 «Умисна неспроможність», ст.. 253 «Фіктивна неспроможність»;
– Австралії керується Актом про корпорації (Corporation Act) та Актом (законом) Австралії про комісію з цінних паперів та інвестицій (Australian Securities and Investments Commission Act), а також спеціальною системою принципів – «Eggleston principles» (1969);
– Китаї: Закон КНР про господарський договір 1981року; Положення про особливі економічні зони провінції Гуандун 1980 року; Закон КНР про зовнішньоекономічний договір 1985 року; закони про приватні підприємства 1988 року; про компанії 1993 року; про господарські товариства 1997 року та цивільним законодавством.

Проаналізовано положення нормативно-правових актів і відповідну правозастосовну практику діяльності іноземних правоохоронних органів та спеціальних органів щодо протидії злочинам, що пов'язані із протиправним заволодінням майном підприємства, установи, організації (рейдерство) в таких країнах: США, Велика Британія, Іспанія, Італія, Німеччина, Австрія, Франція, Ірландія, Норвегія, Швеції, Латвія, Нідерланди, Молдова, Фінляндія, Китай, Японія, Індія, Таїланд та Австралії. Так 87% працівників оперативних підрозділів та 79% слідчих Національної поліції України вказали, що Україна повинна врахувати та впроваджувати законодавчі документи інших країн, що ефективно впливають на мінімізацію вчинення рейдерства.

З огляду на зростаючі ризики безпеки, пов'язані з технологічними інноваціями, відсутністю прозорої економічної політики держави, наявністю тіньової економіки високим рівнем корупції та збільшенням економічних і соціальних проблем, що були викликані пандемію COVID-19, у тому числі в умовах воєнного стану було впроваджено ряд змін до нормативно-правових документів які направлені запобігання та протидію злочинам, що пов'язані із протиправним заволодінням майном підприємства, установи, організації (рейдерство). Отже, враховуючи, що в європейських країнах законодавство виступає за єдність вимог та позитивні зміни у законодавстві зарубіжних країн обґрунтовано варіанти змін і доповнень до ст. 206–2 КК України (щодо криміналізації рейдерства)»Протиправне заволодіння майном підприємства, установи, організації», назву якої запропоновано викласти у такій редакції ст. 206–2 «Рейдерство», об'єднавши всі склади злочинів з посилення відповідальності, враховуючи умисел та розміром шкоди. А також у контексті формування та реалізації державної політики щодо системи заходів протидії рейдерству як інструмента забезпечення національної безпеки держави та гарантування права власності запропоновано авторську редакції проєктів «Стратегії протидії рейдерству до 2035 року» та «Комплексну цільову програму (концепцію) запобігання рейдерству», що полягає в системі загальносоціальних (економічні, правові, ідеологічні, організаційно-управлінські, культурно-виховні, науково-освітні, інформаційні, технічні), спеціально-кримінологічних та індивідуально-профілактичних заходів, що спрямовані на моніторинг і прогнозування криміногенної ситуації в розрізі держави та окремих регіонів та виявлення та усунення детермінантів, які сприяють учиненню рейдерських заходів.

Список використаних джерел:

1. Шубіна С.А. Зарубіжний досвід запобігання привласненню, розтраті майна або заволодіння ним шляхом зловживання службовим становищем у сфері житлово-комунального господарства. Юридичний науковий електронний журнал. URL: http://www.lsej.org.ua/3_2023/98.pdf.

2. Yunin O., Sevruk V., Pavlenko S. Priorities of economic development of Ukraine in the context of european integration. Baltic Journal of Economic Studies. Riga: Publishing House «Baltija Publishing», 2018. Vol. 4. N. 3. P. 358–365.

3. Ополінський А.О. Особливості рейдерства в Україні: інструменти запобігання і протидії протиправному заволодінню майном підприємства, установи, організації. Науковий вісник Ужгородського національного університету. Серія ПРАВО. Випуск 53. Том 2. 2018. С. 74–77.

4. Луговий О.М. Правове регулювання протидії рейдерству в Україна. Національний юридичний журнал: теорія та практика. Січень, № 1 (41), 2020. С. 138–142.

ДО ПИТАННЯ ОБІГУ ЗБРОЇ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Леонід МОГІЛЕВСЬКИЙ
доктор юридичних наук, професор,
заслужений юрист України,
співробітник МВС

З початком повномасштабного вторгнення російської федерації в України, на руках у звичайних українців опинилось багато зброї. Окрім того, суттєво виріс ринок незаконної торгівлі зброєю. Тож, попри значну кількість вогнепальної зброї, ситуація з її обігом в Україні залишається нерегульованою в необхідному для сучасних умов обсязі. Суттєвим недоліком є те, що усі питання, пов'язані із цивільною зброєю, вирішуються виключно через підзаконні нормативні

акти Міністерства внутрішніх справ України. Крім того, в Україні не діє єдиний державний реєстр власників зброї, відсутня чітка класифікація сучасної цивільної вогнепальної зброї [1].

Проблеми у сфері обігу зброї в нашій країні обумовлені тим, що у перші дні війни було видано велику її кількість на руки громадянам, які пішли в сили ТрО і в добровольчі формування територіальної громади. Це ті громадяни, які готові захищати країну. На період воєнного стану вона має в них залишатися, якщо, звичайно, вона не є предметом кримінального розслідування [2]. Як зазначив заступник міністра внутрішніх справ Леонід Тимченко,– «На сьогодні ще не вся зброя, навіть та, що відома поліції, занесена до реєстру. Наразі там зафіксовано 371 тисяча одиниць зброї. Причому число власників цієї зброї не еквівалентне її кількості, оскільки дехто має по кілька одиниць. Отже власників у цьому Реєстрі поки що лише 256 тисяч осіб. Поступово всю інформацію про вогнепальну зброю та її власників актуалізують. Зрештою кожен власник має зареєструвати новопридбану зброю або актуалізувати дані про ту, що вже є. Реєстр було започатковано у 2023 році, і у червні 2026 він має запрацювати на повну силу [3]. Однак, незважаючи на таку здавалося б позитивну тенденцію, після війни, за даними партнерів нашої держави, кількість зброї може бути до трьох мільйонів незареєстрованих стволів. А це в свою чергу може стати суттєвою проблемою для соціальної стабільності у післявоєнній Україні. З огляду на зазначене вище, в умовах сьогодення цілком справедливим буде говорити про те, що визначення порядку обігу в країні цивільної вогнепальної зброї є одним із найбільш складних та, водночас, соціально значимих питань з точки зору оцінки його впливу на стан громадської безпеки.

Втім, забезпеченню законності обігу зброї в Україні в умовах воєнного стану заважає не тільки сам факт ведення бойових дій. Однієї із ключових проблем, яку слід виділити – відсутність саме законодавчого регулювання цієї сфери. Відмітимо, що Верховна Рада України 23 лютого 2022 року опублікувала проєкт закону «Про право на цивільну вогнепальну зброю», метою якого є посилення дотримання режиму законності в питаннях визначення правового режиму власності на зброю, закріплення основних прав та обов'язків громадян і юридичних осіб щодо виробництва, набуття, володіння, розпорядження та використання зброї і боєприпасів, врегулювання інших суспільних відносин, що безпосередньо з цим пов'язані [4]. Втім, за два роки війни реальних кроків у напрямку прийняття цього законопроєкту так зроблено і не було.

Ще однією проблемою, як слушно зазначає В. Санакоєв, є корупція. Автор пише, що «навіть якщо досконалий законопроєкт про легалізацію обігу вогнепальної зброї буде прийнятий Верховною Радою, це не означає, що будь-хто зможе вільно купувати, зберігати та носити при собі пістолет тощо. За такою можливістю стоїть складна процедура отримання ліцензії, підтвердження належного психічного та фізичного стану, створення належних умов зберігання зброї. І, звичайно ж, це буде досить складний та довготривалий процес, отримати кінцевий позитивний результат буде не так уже й легко. Але, як завжди, знайдуться особи, які будуть зацікавлені в тому, щоб обійти встановлену законом процедуру отримання ліцензії та вирішити питання з потрібними дозволами «по блату» або ж за «символічну винагороду» – хабар» [5].

Окрім зазначеного вище, до проблем, обігу зброї в умовах воєнного стану в нашій державі можна віднести наступні: по-перше, відсутність серед населення сформованої культури поводження з вогнепальної зброєю; по-друге, соціальна напруга, обумовлена повномасштабним вторгненням, збіднінням населенням, постійними обстрілами ворога, тощо; по-третє, відсутність реальних та ефективних механізмів контролю за обігом зброї; по-четверте, занадто повільне запровадження електронного реєстру обігу зброєю.

Зауважимо, що існуючі проблеми обігу зброї в умовах воєнного стану в Україні не є не вирішуваними, втім це питання не можна відкладати у «довгий ящик», адже чим довше триває війна, тим більше зброї з'являється на руках у населенням, а відтак зростають ризики її незаконного застосування.

Список використаних джерел:

1. Дерезенко А.В., Іванова А.М., Купилов Е.В. Окремі питання незаконного обігу зброї в умовах воєнного стану: проблеми та шляхи їх вирішення. JURISPRUDENCE / «COLLOQUIM-JOURNAL» № 38 (139) URL: https://cyberleninka.ru/article/n/okremi-pitannya-nezakonnogo-obigu-zbroyi-v-umovah-voennogo-stanu-problemi-ta-shlyahi-yih-virishennya/viewer. (Дата звернення 20.06.2024)
2. Після війни на руках українці можуть мати до трьох мільйонів незареєстрованої зброї. Офційний веб-сайт журналу «Дзеркало тижня» URL: https://zn.ua/ukr/UKRAINE/pislja-vijni-na-rukakh-ukrajintsi-mozhut-mati-do-trokh-miljoniv-nezarejestrovanoji-zbroji-klimenko.html. (Дата звернення 20.06.2024)
3. Марченко Л. В Україні на руках у населення числиться вже понад мільйон одиниць вогнепальної зброї. URL: https://top.today.ua/v-ukrayini-na-rukah-u-naselennya-vzhe-chyslytsya-ponad-miljon-odynyts-vognepalnoyi-zbroyi/.(Дата звернення 20.06.2024)
4. Прийнято за основу проєкт Закону «Про право на цивільну вогнепальну зброю». Верховна Рада України. URL: https://www.rada.gov.ua/news/Novyny/219896.html. (Дата звернення 20.06.2024)
5. Санакоєв Д. Нормативно-правові аспекти врегулювання обігу зброїв умовах воєнного стану. Науковий вісник ДДУВС. 2023. Спеціальний випуск № 2 URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/sp2/NV_spec_2–2023–224–230.pdf. (Дата звернення 20.06.2024)

ЗАПОБІГАННЯ ФІНАНСУВАННЮ ТЕРОРИЗМУ У СВІТЛІ СУЧАСНИХ ВИКЛИКІВ ТА ЗАГРОЗ

Андрій НЕКОЗ
співробітник СБУ

Одним з основних завдань будь-якої держави є протидія злочинності, яка є не лише негативним явищем сьогодення, а й загрозою національній безпеці, охоронюваним суспільним інтересам. У зв'язку із зростанням суспільної небезпеки перед державою постає питання щодо забезпечення ефективної охорони як окремого громадянина, так і всього суспільства в цілому [1, с. 5].

Превентивні заходи для забезпечення миру та безпеки є одними із ключових інструментів політики будь-якої держави. Не є винятком і Україна, адже активізація тероризму та сепаратизму, що виник на початку 2014 року з захопленням АР Крим та активізацією незаконних збройних формувань (за підтримки РФ) на окремих територіях Донецької та Луганської областей, загострив питання ефективного контролю за фінансовими потоками і каналами фінансування терористичних організацій з метою вчасного їх виявлення та блокування. Такі заходи мають сприяти знешкодженню злочинців та запобіганню скоєнню терористичних актів ще на початковому етапі. Складні фінансові схеми, використання інструментів відмивання грошей дають можливість приховати справжнє походження та напрямки руху коштів, що ускладнює процес виявлення дій з фінансування тероризму та вимагає постійного вдосконалення інструментів для протидії такому явищу. Ключову роль у русі грошових потоків в економіці відіграють фінансові установи, відповідно загроза їх використання для здійснення фінансування терористичної діяльності є доволі високою. Впродовж тривалого часу в Україні ризики фінансування тероризму з використанням фінансового сектору розглядалися як другорядні, а сама терористична діяльність – як явище нехарактерне для країни. Проте події останніх років продемонстрували, що сучасний тероризм не обмежений кордонами, має глобальний характер, і часто підтримується як з боку окремих країн, так і недержавних організацій. Методи акумуляції коштів для здійснення терористичної діяльності еволюціонують та урізноманітнюються, і у більшості випадків рух таких коштів здійснюється через фінансовий сектор. Це зумовлює необхідність

розробки регуляторами фінансового ринку і фінансовими установами ефективних інструментів для виявлення грошових потоків, що можуть мати відношення до фінансування тероризму чи розповсюдження зброї масового знищення [2, с. 81].

Терористична загроза в світі сьогодні перебуває на високому рівні. Від неї потерпають як країни, в яких тривають збройні конфлікти (передусім на Близькому Сході та в Африці), так і країни Заходу, які до останнього часу вважалися цілком безпечними з огляду на розвинену систему правоохоронних органів і спецслужб. Протидіяти цій загрозі стає все важче. Міжнародний тероризм – це явище, що не має географічних кордонів і становить небезпеку не лише для окремих країн, а й ставить під сумнів стійкість міжнародного правопорядку і його спроможність протистояти викликам з боку міжнародних терористичних організацій і квазідержавних утворень, які претендують на самостійну роль у системі міжнародних відносин.

Нові тенденції у розвитку міжнародного тероризму створюють додаткові виклики та загрози для національної і міжнародної безпеки та потребують належного і своєчасного реагування. З огляду на це, заходи з удосконалення антитерористичної політики і боротьби з тероризмом як на національному, так і на міжнародному рівнях мають носити перманентний характер навіть за умов низького рівня відповідної загрози. На даний час, зусилля багатьох країн спрямовані на посилення захисту від терористичної загрози [3].

У сучасному світі тероризм розглядають не лише як загрозу правам і свободам людини, а перш за все як суспільно небезпечне діяння, що становить серйозну небезпеку для нормального розвитку демократичних держав, їх зовнішньої та внутрішньої безпеки. Відповідно, визнання тероризму однією з основних загроз національній безпеці України у таких концептуальних документах, як Стратегія національної безпеки України та Стратегія воєнної безпеки України, є цілком послідовним [4, с. 10].

Наразі у багатьох країнах запроваджено та виконуються спеціалізовані програми, спрямовані на недопущення поширення у суспільстві екстремістських поглядів, запобігання втягування молоді до участі у терористичних організаціях, застосовуються процедури амністії окремих осіб, які брали участь в терористичній діяльності, та адаптації їх до мирного співіснування [3].

Загальновідомо, що однією з основних цілей тероризму є викликати паніку серед населення, активізувати політичні процеси, які в подальшому можуть негативно вплинути на розвиток суспільства та розбудову державних інституцій. Останнім часом тероризм трансформується у бізнес модель, що має більш негативні явища ніж традиційні цілі тероризму.

Боротьба з фінансуванням тероризму передбачає насамперед розробку дієвих інструментів для протидії, своєчасного виявлення, припинення фінансуванням терористичної діяльності. Системоутворюючим інструментом є законодавство з питань протидії відмиванню доходів та фінансування тероризму. Варто також зазначити, що впродовж останніх років в Україні сформовано нормативно-правову базу, яка відповідає чинним міжнародним стандартам і є основою для розробки інструментарію з виявлення та зупинення операцій, які можуть бути пов'язані з фінансуванням тероризму чи терористичної діяльності [2, с. 83].

Необхідно також констатувати, що в українській економічній літературі явище фінансування тероризму переважно досліджується у контексті легалізації кримінальних доходів. Водночас на практиці часто зустрічаються випадки, коли фінансування терористичної діяльності здійснюється легальними компаніями чи громадськими або благодійними організаціями, формування фінансових ресурсів яких не викликає питань з точки зору фінансового моніторингу. Навіть виконуючи усі вимоги чинного законодавства, фінансова установа не може бути повністю убезпечена від ймовірності бути причетною до руху фінансових потоків, кінцевими бенефіціарами яких стануть терористичні організації. Тому поглибленого дослідження потребують питання удосконалення системи управління ризиками залучення банків та небанківських установ до фінансування тероризму і терористичних організацій [2, с. 81].

Отже, запобігання фінансуванню тероризму в Україні потребує постійного удосконалення та може бути посилена шляхом прийняттям сучасної нормативно-правової бази, а також приведення її у відповідність до існуючих міжнародних стандартів та практик, постійної взаємодії

уповноважених суб'єктів по боротьбі з тероризмом з правоохоронними органами інших країн і спеціалізованими міжнародними установами, вивчення іноземного досвіду у протидії фінансуванню тероризму та адаптацією такого досвіду до українських реалій.

Список використаних джерел:

1. Луценко Ю.В. Звільнення від кримінальної відповідальності за злочини проти основ національної безпеки України: монографія. Харків: Право. 2015. 200 с.
2. Рисін В.В., Степанова А.В. Інструменти протидії фінансуванню тероризму з використанням фінансових установ. економічна наука. *Економіка та держава. Економічна наука*. 2020. № 6. С. 80–86.
3. Іноземний досвід протидії тероризму: висновки для України. Аналітична записка. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/inozemniy-dosvid-protidii-terorizmu-visnovki-dlya-ukraini (дата звернення: 14.06.2024).
4. Сокуренко В.В. Міжнародне співробітництво України у сфері протидії тероризму: аналіз та перспективи вдосконалення. *Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку*: зб. тез доп. Міжнар. наук.– практ. конф. до 25-річчя ХНУВС (Харків, 18 квіт. 2019 р.). Харків: ХНУВС, 2019. С. 10–12.

АНАЛІЗ ОКРЕМИХ ПОЛОЖЕНЬ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ВОЄННІ ЗЛОЧИНИ (РОЗДІЛ 11.4) ПРОЄКТУ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

Анна ПОЛІТОВА
кандидат юридичних наук, доцент,
доцент кафедри права економіко-правового факультету
Маріупольського державного університету

24 лютого 2024 р. російська федерація продовжила вторгнення на територію України, розпочату ще у лютому 2014 р. Анексія Автономної Республіки Крим, окупація окремих районів Донецької та Луганських областей – це лише порушення територіальної цілісності нашої держави. Проте, розпочатий країною-агресоркою збройний конфлікт супроводжувався та сьогодні продовжує супроводжується низькою зловживань, які можна кваліфікувати як злочини проти людяності, воєнні злочини, злочин агресії та злочин геноциду.

Варто відзначити, що заборона певної поведінки під час збройного конфлікту простежується багато століть, але що стосується концепції воєнних злочинів, то вона розвивалась наприкінці XIX ст.– початку XX ст., коли міжнародне гуманітарне право (відоме також «право збройних конфліктів») було кодифіковано.

Гаазькі конвенції, прийняті у 1899 р. та 1907 р., акцентують увагу на забороні воюючим сторонам використовувати певні засоби і методи ведення війни. Згодом було прийнято кілька інших договорів. Але Женевські конвенції 1864 р. та наступні Женевські конвенції, зокрема чотири Женевські конвенції 1949 р. та два Додаткові протоколи 1977 р., зосереджені на захисті осіб, які не беруть або більше не беруть участі у воєнних діях. Отже, і Гаазькі конвенції, і Женевські конвенції визначають кілька порушень норм, хоча не всі серед них, відносяться до воєнних злочинів. Також варто наголосити, що у міжнародному праві немає єдиного документа, який би кодифікував усі воєнні злочини, але цей перелік можна знайти у міжнародному гуманітарному праві та міжнародному кримінальному праві.

Зауважимо, що Женевські конвенції 1949 р. були ратифіковані всіма державами-членами ООН, тоді як Додаткові протоколи та інші договори з міжнародного гуманітарного права, на превеликий жаль, не досягли такого рівня визнання. Разом з тим, багато норм, що містяться в цих договорах, розглядаються як частина звичаєвого права і, як такі, є обов'язковими для всіх держав та інших сторін конфлікту, незалежно від того, ратифікували вони самі договори чи ні. Окрім того, багато норм міжнародного звичаєвого права застосовуються як у міжнародних, так і у неміжнародних збройних конфліктах, розширюючи таким чином захист, наданий у неміжнародних конфліктах, які регулюються спільною ст. 3 чотирьох Женевських конвенцій та II Додатковим протоколом.

У доповіді Управління Верховного комісара з прав людини щодо ситуації з правами людини в Україні, що охоплює період із 1 грудня 2023 року до 29 лютого 2024 року [1], відзначаються такі порушення:

- загибель щонайменше 429 цивільних осіб (232 чоловіків, 181 жінки, 10 хлопчиків і 6 дівчаток) і поранень 1375 цивільних осіб (717 чоловіків, 576 жінок, 50 хлопчиків і 32 дівчаток). Поміж жертв серед цивільного населення у звітному періоді було 8 працівників засобів масової інформації (поранені 5 жінок і 3 чоловіки), 9 медичних працівників (1 жінка загинула, 5 чоловіків і 3 жінки були поранені) і 7 працівників гуманітарних організацій (2 чоловіки загинули, 4 чоловіки та 1 жінка були поранені)[1];

– Російська Федерація також запровадила свою освітню систему й навчальну програму;
– Російська окупаційна влада здійснює тиск на мешканців окупованої території, щоб змусити їх отримати громадянство і паспорти Російської Федерації, як безпосередньо, шляхом погроз і залякування, так і непрямо, шляхом позбавлення осіб, які не мають російського паспорту, права на отримання основних послуг;
– депортація з окупованої території України до Російської Федерації;
– задокументувало 66 випадків свавільного затримання цивільних осіб (55 чоловіків, 10 жінок, 1 хлопчика) російською владою на окупованій території, причому деякі з цих випадків можуть становити насильницькі зникнення;
– обмеження свободи вираження поглядів;
– катування, жорстоке поводження або сексуальне насильство щодо чоловіків і жінок.

Таким чином, можна відзначити, що під час російсько-українського збройного конфлікту, міжнародне гуманітарне право привертаю значну увагу. Управління Верховного комісара з прав людини фіксує такі порушення не тільки щодо цивільного населення, а й щодо військовополонених, а також випадки застосування російськими військовослужбовцями забороненої зброї. Але чи достатньо цього? Напевно ні, адже притягнення до відповідальності таких осіб має певні проблеми не тільки за національним законодавством, а й міжнародним кримінальним правом.

Важливу роль у міжнародному гуманітарному праві відіграє Римський статут Міжнародного кримінального суду 1998 р. Зокрема, у ст. 8 Статуту визначено перелік воєнних злочинів у міжнародних та неміжнародних збройних конфліктах. Також варто відзначити, що Україна не ратифікувала Римський статут Міжнародного кримінального суду 1998 р., але двічі скористалася своїми прерогативами, щоб визнати юрисдикцію Суду щодо ймовірних злочинів за Римським статутом, які відбуваються на її території, відповідно до статті 12(3) Статуту. Перша заява, подана урядом України, визнала юрисдикцію Міжнародного кримінального суду щодо ймовірних злочинів, скоєних на території України з 21 листопада 2013 року до 22 лютого 2014 року. Друга заява подовжила цей період на безстроковій основі, щоб охопити триваючі передбачувані злочини, скоєні протягом усього періоду. на території України з 20 лютого

[1] З початку повномасштабного збройного нападу Російської Федерації 24 лютого 2022 року через насильство, пов'язане з конфліктом, загинуло щонайменше 10675 цивільних осіб (5079 чоловіків, 3124 жінки, 311 хлопчиків, 250 дівчаток, а також 28 дітей та 1883 дорослих особи, чия стать ще не встановлена), а 20080 цивільних осіб було поранено (6634 чоловіки, 4631 жінка, 595 хлопчиків, 425 дівчаток, а також 291 дитина та 7504 дорослі особи, чия стать ще не встановлена). У цей період УВКПЛ задокументувало також, що в результаті бойових дій було пошкоджено чи зруйновано 1055 закладів освіти та 444 медичні заклади.

2014 року. 28 лютого 2022 року прокурор Міжнародного кримінального суду оголосив, що шукатиме дозволу на відкриття розслідування ситуації в Україні на основі попередніх висновків Офісу, які випливають із його попереднього вивчення, і охоплюють будь-які нові ймовірні злочини, що підпадають під юрисдикцію Суду [2].

Так, покарання винних, що вчинили воєнні злочини на території України як під час гібридного формату збройного конфлікту, так і повномасштабного вторгнення з 24 лютого 2022 р., а також репарації, реституції, компенсація моральних та матеріальних збитків, психологічна реабілітація, увічнення пам'яті загиблих у збройному конфлікті та вибачення винних перед потерпілими – це лише частина того, що відшкодовується.

Важливу роль у розслідуванні воєнних злочинів Російської Федерації в Україні відіграє Департамент протидії злочинам, вчиненим в умовах збройного конфлікту (реорганізовано у 2019 р. з Департаменту нагляду у кримінальних провадженнях щодо злочинів, вчинених в умовах збройного конфлікту), у структурі якого виділено Управління процесуального керівництва досудовим розслідуванням та підтримання публічного обвинувачення у кримінальних провадженнях про злочини, пов'язані із сексуальним насильством. Також воєнні злочини Російської Федерації в Україні розслідують Національна поліція України, Служба безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України. Процесуальне керівництво здійснює Офіс Генерального прокурора України. Органи прокуратури представляють сторону обвинувачення у судах та слідкують за дотриманням законів, міжнародних норм та практик під час документування воєнних злочинів. Таким чином, ці докази можуть бути представлені як в українських, так і в міжнародних судах. Окрім того, 99% усіх воєнних злочинів розслідують і будуть розслідувати в Україні, і винні в цих злочинах також будуть покарані в Україні. Тільки по 1%, або навіть менше, допомагатимуть наші міжнародні партнери, бо їхня функція допоміжна [3].

Так, і напевно ми не скажемо нічого нового у цьому аспекті, що правоохоронні органи сьогодні стикаються з певними проблемами при притягнення до кримінальної відповідальності та кваліфікації таких протиправних діянь. Недосконалість Розділу XX. Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку Закону України про кримінальну відповідальність неодноразово відзначалося не тільки під час наукових заходів, у наукових публікаціях, а також і в певних законопроєктах, наприклад, Проекті Закону про внесення змін до деяких законодавчих актів України щодо імплементації норм міжнародного кримінального та гуманітарного права (реєстр. № 2689 від 27.12.2019).

Сьогодні у робочою групою з питань розвитку кримінального права (Указом Президента України від 7 серпня 2019 р. № 584/2019 «Питання Комісії з питань правової реформи» затверджено Положення про Комісію з питань правової реформи та її персональний склад) підготовлено проєкт Кримінального кодексу України. Він має суттєві відмінності від чинного КК України 2001 р., на яких ми не будемо зупинятися. Відзначимо лише, що Розділ 11.4 присвячено воєнним злочинам. Зупинимося лише на одному прикладі.

Так, стаття 11.4.5 Розділ 11.4 передбачатиме кримінальну відповідальність за серйозне порушення норм міжнародного гуманітарного права у зв'язку з міжнародним збройним конфліктом або збройним конфліктом неміжнародного характеру, не пов'язане зі вбивством, а саме:

«Особа, яка серйозно порушила норми міжнародного гуманітарного права, застосовувані як в міжнародних збройних конфліктах, так і в збройних конфліктах неміжнародного характеру, а саме:

1) катувала людину чи здійснила інше нелюдське поводження щодо неї, що полягає в заподіянні сильних страждань,

2) заподіяла тяжке насильство щодо людини,

3) посягнула на людську гідність, зокрема образила, принизила іншу людину, що перебувала під захистом міжнародного гуманітарного права, чи вчинила щодо неї чи щодо померлої людини інше діяння, що з урахуванням культурної приналежності потерпілої людини завдало шкоди людській гідності,

4) захопила заручника,

5) здійснила незаконну депортацію, переміщення чи незаконне ув'язнення цивільних осіб з причин, пов'язаних з конфліктом, якщо необхідність у цьому не була викликана вимогами безпеки цивільних осіб чи причинами воєнного характеру,

6) зґвалтувала, звернула в сексуальне рабство, примусила до проституції, примусової вагітності, примусової стерилізації чи іншої форми сексуального насильства, що становить серйозне порушення статті 3, спільної для чотирьох Женевських конвенцій,

7) набрала чи завербувала дітей віком до п'ятнадцяти років до складу національних збройних сил або груп чи використала таких дітей для активної участі в бойових діях,

8) спричинила людині, яка перебуває під владою протилежної сторони конфлікту, фізичне каліцтво або здійснила щодо неї медичний (біологічний) чи науковий експеримент, не обґрунтований ні потребою в її медичному, стоматологічному лікуванні чи лікарняному догляді, ні її інтересами,

9) використала голод цивільного населення як метод ведення війни шляхом позбавлення населення предметів, необхідних для виживання, у тому числі створила перешкоди для надання допомоги, передбаченої в Женевських конвенціях,

10) спрямувала напад на цивільне населення чи на окремих цивільних осіб, що не беруть безпосередньої участі у воєнних діях,

11) спрямувала напад на цивільний об'єкт,

12) спрямувала напад на незахищені і такі, що не є воєнними цілями, місто, село, помешкання чи будівлю або обстріляла їх,

13) спрямувала напад з розумінням того, що він призведе до загибелі чи поранення цивільних осіб або завдасть шкоди цивільному об'єкту чи масштабної, тривалої і серйозної шкоди навколишньому природному середовищу, яка буде явно надмірною порівняно з конкретною та безпосередньо очікуваною загальною військовою перевагою,

14) застосувала засоби ведення війни, заборонені міжнародним гуманітарним правом,

15) спрямувала напад на установку чи споруду, яка містить небезпечну силу, що завідомо могло призвести до загибелі або поранення осіб, які належать до цивільного населення, чи завдати надмірної шкоди цивільному об'єкту,

16) заявила про те, що пощади не буде,

17) віроломно поранила особу, зазначену в підпункті (в) пункту 13 статті 11.4.1 цього Кодексу,

18) використала присутність цивільної особи чи іншої особи, що перебуває під захистом міжнародного гуманітарного права, для захисту певного пункту, району чи збройних сил від воєнних дій,

19) використала рухому чи нерухому цінність, яка перебуває під посиленим захистом міжнародного гуманітарного права, чи прилеглі до неї місця для підтримки бойових дій,

20) застосувала зброю, боєприпаси чи матеріали або методи ведення війни, які спричиняють надмірні ушкодження чи непотрібні страждання або є невибірковими за своєю суттю,

21) спрямувала напад на будівлю, матеріал, медичну установу, транспортний засіб або персонал, що використовують згідно з міжнародним правом емблему чи розпізнавальний знак, встановлені міжнародним гуманітарним правом, або позначені такою емблемою чи знаком,

22) неналежно використала зазначені відмітну емблему чи розпізнавальний знак, піддавши небезпеці особу чи осіб,

23) незаконно, безглуздо та в широких масштабах знищила чужу власність, якщо це не було викликано воєнною необхідністю,

24) заволоділа чужою власністю у місті чи іншому населеному пункті, якщо це не було викликано воєнною необхідністю,

25) заволоділа цінністю, яка перебуває під захистом міжнародного гуманітарного права,

26) спрямувала напад на цінність, яка перебуває під захистом міжнародного гуманітарного права,

27) вчинила акт вандалізму щодо цінності, яка перебуває під захистом міжнародного гуманітарного права, або

28) спрямувала напад на персонал, об'єкт, матеріал, підрозділ чи транспортний засіб, задіяний в наданні гуманітарної допомоги або в місії з підтримання миру відповідно до Статуту Організації Об'єднаних Націй, доки вони мають право на захист міжнародного гуманітарного права, яким користуються цивільні особи чи цивільні об'єкти,– вчинила злочин 7 ступеня» [4].

Отже, відзначимо, що у цій статті мають місце помилки: використовується двічі нумерація 10, відсутнє 27 – при переліченні ознак об'єктивної сторони цього складу злочину. Також має місце відсилочний характер до інших статей та міжнародних документів, що може бути не зовсім зручно при кваліфікації таких діянь, а використання словосполучення «міжнародного гуманітарного права» може бути не зрозумілим пересічному громадянину та потребує роз'яснення. Вважаємо, що зроблені нами висновки потребують подальшого наукового дослідження та більш точної аргументації.

Список використаних джерел:

1. Доповідь щодо ситуації з правами людини в Україні. 1 грудня 2023 року – 29 лютого 2024 року. URL: https://ukraine.un.org/sites/default/files/2024–04/2024–03–26-ohchr-38th-periodic-report-ukr.pdf (Дата звернення 21.06.2024)

2. Ukraine. Situation in Ukraine. ICC-01/22. URL: https://www.icc-cpi.int/situations/ukraine (Дата звернення 21.06.2024).

3. Керівник департаменту війни: 99% усіх воєнних злочинів розслідують і розслідуватимуть в Україні URL: https://interfax.com.ua/news/general/926529.html (Дата звернення 21.06.2024).

4. Текст проєкту нового Кримінального кодексу України/Draft of the new Criminal Code of Ukraine. URL: https://newcriminalcode.org.ua/criminal-code (Дата звернення 21.06.2024).

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ЗАПОБІЖНИХ ЗАХОДІВ У ПРОВАДЖЕННЯХ ЩОДО КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ

Ігор РОГАТЮК
доктор юридичних наук, професор,
заслужений юрист України,
співробітник СБУ
Костянтин АНТОНОВ
співробітник СБУ

У контексті необхідності протидії колабораціонізму, варто ретельно розглянути застосування запобіжних заходів до осіб, які підозрюються або обвинувачуються у такій діяльності. Це актуальне завдання кримінального процесу стикається з ускладненими викликами сучасності. Колабораціонізм, що становить загрозу національній безпеці, суверенітету та міжнародному праву, може призвести до серйозних наслідків, таких як вчинення злочинів проти людства, впливу сил ворога на політику країни, створення соціальної напруженості та ін. Отже, розумне й ефективне застосування запобіжних заходів при розслідуванні кримінальних проваджень за відповідною класифікацією стає необхідністю у збереженні національної безпеки та міжнародної стабільності.

Під час дії воєнного стану, особам, які підозрюються або обвинувачуються за статтею 111–1 Кримінального кодексу України, за наявності ризиків, зазначених у статті 177 КПК України, слідчий суддя та суд можуть обрати лише єдиний безальтернативний запобіжний захід: три-

мання під вартою. Відповідні зміни були внесені до статті 176 КПК України на підставі Закону України від 14.04.2022 р. № 2198-IX шляхом доповнення її частиною шостою. Також, частину четверту статті 183 КПК України доповнили абзацом восьмим, який надає право слідчому судді та суду, обираючи особі запобіжний захід у вигляді тримання під вартою у кримінальних провадженнях щодо колабораційної діяльності, не визначати розмір застави [1]. Такий порядок безальтернативного обрання запобіжних заходів до осіб, що підозрюються або обвинувачуються у вчиненні колабораціонізму, застосовується саме на період дії правового режиму воєнного стану.

Заходи запобіжного характеру не мають на меті накладення покарання за вчинений злочин. Їх головна ціль полягає в забезпеченні належної процесуальної поведінки особи, яка є підозрюваною або обвинуваченою. При застосуванні запобіжних заходів до особи завжди необхідно керуватися наступними правовими принципами, які є універсальними і мають застосовуватися у будь-якій країні, де діє принцип верховенства права:

1. Принцип презумпції невинуватості гарантує, що кожна особа вважається невинуватою у вчиненні злочину, поки її вину не буде встановлено обвинувальним вироком суду (згідно зі ст. 62 Конституції України та ч. 2 ст. 6 Конвенції про захист прав людини і основоположних свобод).

2. Принцип презумпції свободи гарантує кожній особі свободу та особисту недоторканність (закріплено у ст. 29 Конституції України та ст. 5 Конвенції).

3. Принцип імперативної поваги до людської гідності гарантує кожній особі повагу до її гідності. Заборона жорстокого поводження є абсолютною (згідно зі ст. 3 Конвенції).

У 2014 році законодавець вже намагався закріпити безальтернативність обрання запобіжного заходу у вигляді тримання під вартою для осіб, підозрюваних або обвинувачених у злочинах проти національної та громадської безпеки України [2]. Проте Конституційний суд у 2019 році визнав це положення частини 5 статті 176 КПК неконституційним і зазначив, що такий підхід не відповідає міжнародній практиці. Суд наголосив, що формальне судове рішення не повинно нівелювати мету та суть правосуддя (Рішення від 25 червня 2019 року 7-р/2019), та підкреслив, що суддя, враховуючи обставини справи, повинен мати можливість застосовувати більш м'які запобіжні заходи, які визначені на законодавчому рівні. Відсутність такої можливості обмежує право особи на свободу та особисту недоторканність, порушуючи принцип верховенства права [3].

Слід відзначити, що право на свободу не є абсолютним і може бути обмежене відповідно до вимог домірності (пропорційності) та суспільної необхідності. Ці обмеження повинні мати легітимну мету, бути обумовлені суспільною необхідністю досягнення цієї мети, пропорційними та обґрунтованими [4].

В умовах повномасштабної агресії рф, легітимною метою доповнення статті 176 КПК України частиною шостою є суспільна необхідність у захисті суверенітету і територіальної цілісності України, а також забезпеченні її державної (національної) безпеки, згідно зі статтею 17 Конституції України. У цьому контексті застосування ізоляційних запобіжних заходів до осіб, які співпрацюють із ворогом в його інтересах, є легітимними засобами досягнення вказаної мети.

Як приклад, в травні 2024 року СБУ затримано колаборанта, який співпрацював з рф під час окупації Херсона. Тоді він «служив» у російській катівні, яку рашисти облаштували на базі захопленої на той час Дар'ївської виправної колонії № 10.Там він перебував на «посаді» охоронця окупаційного об'єкта, до якого рашисти звозили репресованих місцевих жителів, зокрема проукраїнських активістів. Після звільнення правобережної Херсонщини колаборант певний час переховувався, а згодом мобілізувався до українського війська, де сподівався уникнути правосуддя. Співробітники СБУ задокументували злочинну діяльність фігуранта та його спроби сховатися від правосуддя в одній із військових частин на півдні України. За даними слідства, ворожим поплічником виявився мешканець Миколаївщини, ідеологічний прихильник рашизму. На початку повномасштабного вторгнення він підтримав окупантів, за що був

призначений охоронцем російської катівні. На підставі зібраних доказів слідчі Служби безпеки повідомили затриманому про підозру за ч. 7 ст. 111–1 Кримінального кодексу України. Зловмиснику обрано запобіжний захід тримання під вартою [5].

Необхідність використання тримання під вартою під час дії воєнного стану до колаборантів, є одним з наслідків відступу України від своїх зобов'язань, що здійснив законодавець згідно зі статтею 15 Конвенції про захист прав людини і основоположних свобод. Україна повідомила Генерального секретаря Ради Європи про відповідну дерогацію, обумовлену масштабною неспровокованою військовою агресією з боку російської федерації. Цей крок дозволив дотриматися формальних умов легітимності обмеження права на свободу та особисту недоторканність на період дії воєнного стану в українському законодавстві [6].

Потрібно зазначити, що безальтернативність запобіжних заходів не означає немотивованість судового рішення. Відсутність обґрунтованої підозри або ризиків невиконання процесуальних обов'язків зазвичай призводить до відмови в обранні запобіжного заходу.

Підсумовуючи викладене слід зазначити, що для відновлення справедливості та уникнення вибіркового правосуддя дуже важливо притягнути до передбаченої законом відповідальності всіх осіб, причетних до вчиненні колабораційної діяльності. Не менш важливим для України, як правової держави, в процесі здійснення кримінального переслідування є забезпечення таких основоположних засад як рівність та повага до людської гідності, а також дотримання інших прийнятих на себе зобов'язань щодо захисту прав людини. Саме тому рішення по обиранню запобіжного заходу у кримінальних провадженнях щодо колабораційної діяльності потребує обов'язкового мотивування згідно з базовими правовими принципами та міжнародними стандартами.

Список використаних джерел:

1. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки: Закон України від 14.04.2022 р. № 2198-IX. URL: https://zakon.rada.gov.ua/laws/show/2198–20#Text (дата звернення: 04.06.2024).

2. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо невідворотності покарання за окремі злочини проти основ національної безпеки, громадської безпеки та корупційні злочини: Закон України від 07.10.2014 р. № 1689-VII. URL: https://zakon.rada.gov.ua/laws/show/1689–18#Text (дата звернення: 04.06.2024).

3. Рішення Конституційного Суду України у справі за конституційними скаргами Ковтун Марини Анатоліївни, Савченко Надії Вікторівни, Костоглодова Ігоря Дмитровича, Чорнобука Валерія Івановича щодо відповідності Конституції України (конституційності) положення частини п'ятої статті 176 Кримінального процесуального кодексу України: Рішення Конституційного суду України від 25.06.2019 № 7-р/2019. URL: https://zakon.rada.gov.ua/laws/show/v007p710–19#Text (дата звернення: 04.06.2024)

4. Рішення Конституційного Суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) положення третього речення частини першої статті 13 Закону України «Про психіатричну допомогу»: Рішення Конституційного суду України від 01.06.2016 № 2-рп/2016. URL: https://zakon.rada.gov.ua/laws/show/v002p710–16#n23 (дата звернення: 04.06.2024).

5. СБУ затримала ексохоронця російської катівні, який намагався сховатися у лавах ЗСУ. Служба безпеки України. URL: https://ssu.gov.ua/novyny/sbu-zatrymala-eksokhorontsia-rosiiskoi-kativni-yakyi-namahavsia-skhovatysia-u-lavakh-zsu (дата звернення: 04.06.2024).

6. Про відступ України від зобов'язань за Конвенцією про захист прав людини і основоположних свобод: заява Постійного представництва України при Раді Європи від 28.02.2022 р. № 31011/32–017–3. URL: https://rm.coe.int/1680a5b0b0 (дата звернення: 04.06.2024).

ОСНОВНІ НАПРЯМИ ДІЯЛЬНОСТІ СУБ'ЄКТІВ СУДОВО-ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ З ІНТЕГРАЦІЇ ДО ЄВРОПЕЙСЬКОГО СУДОВО-ЕКСПЕРТНОГО ПРОСТОРУ

Андрій СВІНЦИЦЬКИЙ
кандидат юридичних наук,
заслужений юрист України,
в.о. директора Науково-дослідного центру
незалежних судових експертиз
Міністерства юстиції України

Зважаючи на зростаючий науковий та практичний інтерес до питання співробітництва національних суб'єктів судово-експертної діяльності з представниками експертної спільноти країн Європейського Союзу, активізацією євроінтеграційних процесів та адаптації національного законодавства в сфері експертного забезпечення правосуддя до актів права Європейського Союзу (acquis ЄС), актуалізується питання щодо вироблення нових наукових пропозицій для пошуку ефективних шляхів інтеграції до Європейського судово-експертного простору. У цих тезах доповіді пропонуємо проаналізувати існуючі підходи національних суб'єктів судово-експертної діяльності з реалізації євроінтеграційних завдань та сформулювати авторське бачення щодо вирішення цього питання.

Варто почати з аналізу законодавчих передумов щодо міжнародної діяльності суб'єктів судово-експертної діяльності. Відповідно до ст. 24 Закону України «Про судову експертизу» «…державні спеціалізовані установи, що виконують судові експертизи, користуються правом встановлювати міжнародні наукові зв'язки з установами судових експертиз, криміналістики тощо інших держав, проводити спільні наукові конференції, симпозіуми, семінари, обмінюватися стажистами, науковою інформацією й друкованими виданнями та здійснювати спільні видання в галузі судової експертизи та криміналістики». Так, на практиці суб'єкти судово-експертної діяльності зазвичай укладають угоди про співробітництво з питань наукової та судово-експертної діяльності, залучають в якості співорганізаторів (учасників, спікерів) представників експертної спільноти до участі у міжнародних наукових конференціях та інших наукових заходів, організовують спільні навчання та стажування судових експертів тощо.

До основних форм міжнародної діяльності вчені також відносять «…участь у міжнародних проєктах, акредитацію лабораторій державних спеціалізованих установ, а також співробітництво з Європейською мережею судово-експертних установ» [с. 60]. Погоджуємось з позицією Н. Клименко, що «…національна судова експертиза не може існувати ізольовано, тобто тільки в межах окремої держави, оскільки вона активно не виконуватиме свої функції забезпечення правоохоронної діяльності поза інтеграцією з міжнародною спільнотою» [16, с. 131].

Відзначимо, що сфера експертного забезпечення правосуддя України активно налагоджує співробітництво з експертною спільнотою країн-ЄС про що свідчить активна діяльність національних суб'єктів судово-експертної діяльності у роботі Європейської мережі судово-експертних установ (European Network of Forensic Science Institutes; далі – ENFSI). Так, згідно з інформації опублікованої на офіційному сайті членами ENFSI є Державний науково-дослідний експертно-криміналістичний центр МВС України (ДНДЕКЦ), Київський науково-дослідний інститут судових експертиз Міністерства юстиції України, Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України (ІСТЕ СБУ). Втім, варто наголосити, що судові експерти, які не є працівниками державних спеціалізованих установ наразі не входять до складу жодної експертної робочої групи

ENFSI (Expert Working Groups), хоча, відповідно до статуту ENFSI передбачена можливість особистої участі окремих експертів у складі відповідних робочих груп.

Повністю підтримуємо точку зору О. Лінника та Л. Омельчук, що «…інтеграційні процеси в судово-експертної діяльності сприяють гармонізації та вдосконаленню експертного національного законодавства, розвитку теоретичних основ експертних досліджень, виробленню єдиних методичних рекомендацій з їхнього проведення, вдосконаленню експертної діяльності, підвищенню професійної майстерності працівників судово-експертних установ, міжнародному визнанню національних експертних висновків» [19, с. 240]. Має рацію О. Агапова, яка досліджувала питання розвитку Європейського судово-експертного простору та правові засади розвитку судово-експертної діяльності у країнах Європейського Союзу. Так, вчена акцентувала увагу на важливості розроблення керівного документу державної політики, як то «…концепції розвитку сфери експертного забезпечення правосуддя в Україні».

Ґрунтуючись на нормативно-правовому та доктринальному аналізі питання інтеграції до Європейського судово-експертного простору вважаємо, що до напрямів діяльності національних суб'єктів судово-експертної діяльності слід зарахувати такі:

1. Розроблення документів стратегічного характеру, або включення до діючих керівних документів державної політики положень щодо активізації роботи державних спеціалізованих установ у напряму входження до Європейського простору судово-експертної діяльності.

2. Активізація міжнародного напрямку діяльності суб'єктів судово-експертної діяльності через створення відділів міжнародної діяльності, або введення посад фахівців-міжнародників, здатних компетентно сприяти входженню установи до Європейського простору судово-експертної діяльності.

3. Впровадження практичних спеціалізованих курсів із залученням експертної спільноти країн-ЄС з метою реалізації євроінтеграційного завдання та злиття з Європейським простором судово-експертної діяльності.

4. Підвищення мовних компетентностей судових експертів та працівників державних спеціалізованих установ для вільного спілкування та налагодження співробітництва з представниками експертної спільноти ЄС.

5. Здійснення заходів щодо членства та участі у роботі Європейської мережі судово-експертних установ (European Network of Forensic Science Institutes).

Запропонований перелік напрямів діяльності не є вичерпним. На наше глибоке переконання, у сучасних євроінтеграційних умовах оперативність реагування на зміни в експертному середовищі, впровадження нових та інноваційних підходів до організації судово-експертної діяльності є факторами впливу на розвиток сфери експертного забезпечення правосуддя.

Список використаних джерел:

1. Про судову експертизу: Закон України від 25 лютого 1994 р. No 4038–XII. Відомості Верховної Ради України. 1994. No 28. Ст. 232.

2. Агапова О.В. Класифікація напрямів діяльності у сфері експертного забезпечення / О.В. Агапова // Держава та регіони. Серія: Право.– 2020.– № 3.– С. 58–63.– Режим доступу: http://nbuv.gov.ua/UJRN/drp_2020_3_12.

3. Клименко Н.І., Купрієвич О.А. Міжнародне співробітництво судово-експертних установ. Вісник кримінального судочинства. 2015. No 4. С. 130–134.

4. Линник О.В., Омельчук Л.В. Актуальність вступу України до Міжнародних судово-екс-пертних мереж. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). Вип. 2–3 (6–7). 2017. С. 236–241.

5. Агапова, О. В. (2020). Щодо необхідності розробки концепції розвитку сфери експертного забезпечення правосуддя в україні. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право», (29), 162–168. https://doi.org/10.26565/2075–1834–2020–29–21.

ПРОБЛЕМНІ ПИТАННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА НЕЗАКОННЕ ВИКОРИСТАННЯ З МЕТОЮ ОТРИМАННЯ ПРИБУТКУ ГУМАНІТАРНОЇ ДОПОМОГИ

Антон СТОЛІТНІЙ
доктор юридичних наук, професор,
професор Національного юридичного
університету імені Ярослава Мудрого

Законом № 2155-IX від 24.03.2022 Кримінальний кодекс України доповнено новою статтею 201^2 «Незаконне використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги» [1], в якій такі діяння «прив'язані» до вартості гуманітарної допомоги (ч. 1 – значний розмір або що перевищує 350 нмдг (434,2 тис. грн)).

Слід зазначити, що предметом вказаного злочину є гуманітарні товари, разом з тим, ряд кримінальних проваджень, предметом розслідування яких є незаконне заволодіння товарами вказаної категорії, кваліфіковані не за спеціальною нормою, а саме за ст. 201–2 КК України.

Вказане обумовлено тим, що даний склад злочину є матеріальним, а отже його об'єктивна сторона передбачає діяння у вигляді незаконного заволодіння гуманітарними товарами, благодійними пожертвами або безоплатною допомогою, незаконного розпорядження з метою отримання прибутку (продаж, укладення інших правочинів щодо розпорядження майном, з метою отримання прибутку, вчинені у значному розмірі) та причинний зв'язок між ними.

Тобто нововведена норма, якою доповнено КК України, є перевантаженою за своєю конструкцією та важко застосованою, у тому числі через процедуру документування. Наприклад, особа незаконно заволоділа гуманітарною допомогою, яку в подальшому не реалізує, а зберігає декілька місяців, для доведення даного злочину: по-перше повинне відбуватись документування всього періоду зберігання, по-друге, незрозуміло чи взагалі буде вказана особа реалізовувати даний гуманітарні товари в подальшому.

Прикладом наведеного є кримінальне провадження зареєстроване органами правопорядку Полтавської області у березні 2022 року за ч. 3 ст. 191 КК України за фактом привласнення гуманітарної допомоги громадянами С. 1 та С. 2. Зокрема, вказані особи будучи членами добровольчого формування Н-ської територіальної громади № 1 в м. Н-ськ, без відома керівництва цього формування, домовились і отримали для нього (добровольчого формування) товари гуманітарної допомоги, які їм надала БО «Західно-регіональна благодійна організація міжнародного центру впровадження програм Юнеско».

На час отримання товарів у місті Львів, громадяни С. 1 та С. 2, були виключеними зі складу вказаного добровольчого формування, незважаючи на це отримали та привласнили гуманітарні товари, які зберігали за місцем проживання родичів, де були виявлені та вилучені під час проведення обшуку в межах досудового розслідування (загалом 160 ящиків з продуктами харчування та засобами гігієни).

Відповідно до п. 6 ч. 2 ст. 242 КПК України, слідчий або прокурор зобов'язані забезпечити проведення експертизи щодо визначення розміру матеріальних збитків, якщо потерпілий не може їх визначити та не надав документ, що підтверджує розмір такої шкоди, розміру шкоди немайнового характеру, шкоди довкіллю, заподіяного кримінальним правопорушенням [2].

Відповідно до ст. 1 Закону України «Про судову експертизу», судова експертиза – це дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів,

явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду [3].

Відповідно до п. 1.2, розділу IV Інструкції про призначення та проведення експертиз та експертних досліджень, Основними завданнями товарознавчої експертизи є: визначення вартості товарної продукції; визначення належності товарів до класифікаційних категорій, які прийняті у виробничо-торговельній сфері; визначення характеристик об'єктів дослідження відповідно до вимог Українського класифікатора товарів зовнішньої економічної діяльності; визначення змін показників якості товарної продукції; установлення способу виробництва товарної продукції: промисловий чи саморобний, підприємства-виробника, країни-виробника; визначення відповідності упакування і транспортування, умов і термінів зберігання товарної продукції до вимог чинних правил [4].

Як наслідок у вказаному кримінальному провадженні, яке розслідувались слідим органом Полтавського регіону, призначено та проведено 274 товарознавчих експертизи товарів гуманітарної допомоги з метою визначення їх вартості.

Необхідність проведення такої кількості експертиз обумовлена тим, що товари в рамках гуманітарної допомоги мають різні назви, виробників (відносяться до різних груп товарів) та при митному оформленні не оцінюються (відсутнє документальне підтвердження їх вартості), оскільки товари (предмети), що ввозяться (пересилаються) як гуманітарна допомога, підлягають першочерговому безкоштовному спрощеному декларуванню митним органам відповідними установами та організаціями незалежно від форми власності [5].

До проведення вказаних експертиз було залучено 11 експертів. Тільки після проведення всіх експертиз, які тривали з червня по жовтень 2022 року, вказаним особам повідомлено про підозру за ч. 4 ст. 191 КК України та 22.03.2023 обвинувальний акт стосовно зазначених осіб направлено до суду.

Про проблеми документування, у тому числі, свідчать статистичні дані за ст. 201–2 КК України надані Офісом Генерального прокурора 28.04.2024.

Так, протягом 2023 (2024) року зареєстровано правопорушень: ч. 1–2 (0); ч. 2–4 (1); ч. 3–243 (42). Закрито кримінальних проваджень: ч. 1 ст. 201–2 – 1 (0); ч. 2 ст. 201–4 (0); ч. 3–57 (0). Скеровано до суду: ч. 1–0 (0); ч. 2–0 (0); ч. 3–25 (1).

Виходячи з наданих Офісом Генерального прокурора даних, протягом минулого року правоохоронними органами держави виявлено 249 злочинів щодо незаконне використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги, що становить менше 10 злочинів на регіон, з яких до суду скеровано лише 10% (25). В цьому році з 43 виявлених злочинів до суду скеровано 1, тобто (2,3%).

Про актуальність та проблемність даного питання свідчить постанова Верховної ради України від 20.09.2022 Про утворення Тимчасової слідчої комісії Верховної Ради України з питань розслідування можливих порушень законодавства України у сфері отримання, розподілу, транспортування, зберігання, використання за цільовим призначенням гуманітарної та іншої допомоги, а також неефективного використання державного майна, яке може бути використане для тимчасового розміщення внутрішньо переміщених осіб та забезпечення інших потреб держави [6].

Відповідно до п. 7 звіту Тимчасової слідчої комісії Верховної Ради України з питань розслідування можливих порушень законодавства України у сфері отримання, розподілу, транспортування, зберігання, використання за цільовим призначенням гуманітарної та іншої допомоги, а також неефективного використання державного майна, яке може бути використане для тимчасового розміщення внутрішньо переміщених осіб та забезпечення інших потреб держави від 21 вересня 2023 року № 3395-IX, Національна поліція України повідомила (лист № 4310/01/24–2023 від 04.05.2023), що з початку повномасштабного вторгнення російської федерації на територію України слідчими підрозділами поліції розпочато досудове розслідування в 746 кримінальних провадженнях за фактами незаконних дій з гуманітарною допомогою, благодійними пожертвами та безоплатною допомогою. У вчиненні 157 кримінальних правопору-

шень зазначеної категорії 135 особам повідомлено про підозру, обвинувальні акти в 57 таких кримінальних провадженнях направлено до суду [6].

Про виконану роботу на цьому напрямку також поінформували Бюро економічної безпеки України відзначило (п. 10), Національне антикорупційне бюро України (п. 11), Державне бюро розслідувань (п. 12), Служба безпеки України (п. 13) [5].

Разом з тим, незважаючи на проблемність кваліфікації даного виду злочину, різниці в показниках та ряд інших процесуальних складнощів, відповідно до п. 14 Звіту від Офісу Генерального прокурора інформація за результатами розгляду попереднього звіту Комісії на виконання п. 4 Постанови Верховної Ради України від 11 квітня 2023 року № 3044-IX не надходила [6].

Більш того, відповідно до відповіді Офісу Генерального прокурора на інформаційний запит від 30.04.2024, у 2023 та 2024 роках Генеральним прокурором координаційні наради безпосередньо із зазначених питань не проводились.

Враховуючи окреслену проблематику, доцільно переглянути методику проведення товарознавчої експертизи щодо можливості проведення в рамках кримінального провадження єдиної експертизи по всіх групах товарів, які відносяться до гуманітарного вантажу. Окрім того, на сьогодні потребує перегляду підхід до координаційної діяльності Генерального прокурора з питань виявлення, документування, притягнення до кримінальної відповідальності за незаконні оборутки з гуманітарною допомогою, а також обліку такої роботи.

Список використаних джерел:

1. Кримінальний кодекс України. Режим доступу: https://zakon.rada.gov.ua/laws/show/2341–14#Text. (дата звернення: 18.06.2024)

2. Кримінальний процесуальний кодекс України. Режим доступу: https://zakon.rada.gov.ua/laws/show/4651–17#Text. (дата звернення: 18.06.2024)

3. Закону України «Про судову експертизу». Режим доступу: https://zakon.rada.gov.ua/laws/show/4038–12#Text. (дата звернення: 18.06.2024)

4. Інструкції про призначення та проведення експертиз та експертних досліджень, затверджена Наказом Міністерства Юстиції України 08.10.1998 № 53/5. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0705–98?find=1&text=%D1%82%D0%BE%D0% B2%D0%B0%D1%80%D0%BE%D0%B7%D0%BD%D0%B0%D0%B2%D1%87%D0%B0#w1_3. (дата звернення: 18.06.2024)

5. Закон України «Про гуманітарну допомогу». Режим доступу: https://zakon.rada.gov.ua/laws/show/1192–14?find=1&text=склад#w1_2. (дата звернення: 18.06.2024)

6. Постанова Верховної ради України від 20.09.2022 Про утворення Тимчасової слідчої комісії Верховної Ради України з питань розслідування можливих порушень законодавства України у сфері отримання, розподілу, транспортування, зберігання, використання за цільовим призначенням гуманітарної та іншої допомоги, а також неефективного використання державного майна, яке може бути використане для тимчасового розміщення внутрішньо переміщених осіб та забезпечення інших потреб держави. https://zakon.rada.gov.ua/laws/show/2603-IX#Text. (дата звернення: 18.06.2024).

ОКРЕМІ АСПЕКТИ УДОСКОНАЛЕННЯ СУДОВО-ЕКСПЕРТНОЇ ДВЯЛЬНОСТІ

Світлана СУХАРЄВА
судовий експерт лабораторії
економічних видів досліджень
Науково-дослідного центру судової
експертизи у сфері інформаційних
технологій та інтелектуальної власності
Міністерства юстиції України

Відповідно до статті 1 Закону України «Про судову експертизу» від 25 лютого 1994 року № 4038-XII (далі- Закон № 4038-XII) судова експертиза – це дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду.

Відповідно до статті 15 Закону № 4038-XII витрати на проведення судових експертиз науково-дослідними установами Міністерства юстиції України та судово-медичними і судово-психіатричними установами Міністерства охорони здоров'я України у цивільних і господарських справах відшкодовуються в порядку, передбаченому чинним законодавством.

Проведення інших експертних досліджень і обстежень державними спеціалізованими установами здійснюється за рахунок замовника.

Постановою Кабінету Міністрів України від 27 липня 2011 р. № 804 затверджено «Перелік платних послуг, що надаються науково-дослідними установами судових експертиз Міністерства юстиції».

Однак, на сьогодні не існує Методик та Методичних рекомендацій з питання визначення вартості нормо години під час проведення судових експертиз та наданні платних послуг науково-дослідними установами судових експертиз Міністерства юстиції.

Слід зазначити, що відповідно до статті 13 Бюджетного кодексу України від 8 липня 2010 року № 2456-VI бюджет може складатися із загального та спеціального фондів.

Складовими частинами спеціального фонду бюджету є:

1) доходи бюджету (включаючи власні надходження бюджетних установ), які мають цільове спрямування;

2) видатки бюджету, що здійснюються за рахунок конкретно визначених надходжень спеціального фонду бюджету (у тому числі власних надходжень бюджетних установ);

3) кредитування бюджету (повернення кредитів до бюджету з визначенням цільового спрямування та надання кредитів з бюджету, що здійснюється за рахунок конкретно визначених надходжень спеціального фонду бюджету);

4) фінансування спеціального фонду бюджету.

Власні надходження бюджетних установ отримуються додатково до коштів загального фонду бюджету і включаються до спеціального фонду бюджету. При цьому надходження бюджетних установ у вигляді майна (активів) в натуральній формі, отримане від інших бюджетних установ, які відповідно до законодавства виконують функції з управління об'єктами державної (комунальної) власності, у межах відповідного бюджету, не є власними надходженнями таких бюджетних установ.

Власні надходження бюджетних установ поділяються на такі групи:

– перша група – надходження від плати за послуги, що надаються бюджетними установами згідно із законодавством;
– друга група – інші джерела власних надходжень бюджетних установ.

У складі першої групи виділяються такі підгрупи:

– підгрупа 1 – плата за послуги, що надаються бюджетними установами згідно з їх основною діяльністю;

– підгрупа 2 – надходження бюджетних установ від додаткової (господарської) діяльності;
– підгрупа 3 – плата за оренду майна бюджетних установ, що здійснюється відповідно до Закону України «Про оренду державного та комунального майна»;
– підгрупа 4 – надходження бюджетних установ від реалізації в установленому порядку майна (крім нерухомого майна).

У складі другої групи виділяються такі підгрупи:
– підгрупа 1 – благодійні внески, гранти та дарунки;
– підгрупа 2 – надходження, що отримують бюджетні установи від підприємств, організацій, фізичних осіб та від інших бюджетних установ для виконання цільових заходів, у тому числі заходів з відчуження для суспільних потреб земельних ділянок та розміщених на них інших об'єктів нерухомого майна, що перебувають у приватній власності фізичних або юридичних осіб;
– підгрупа 3 – надходження, що отримують державні і комунальні заклади професійної (професійно-технічної), фахової перед вищої та вищої освіти від розміщення на депозитах тимчасово вільних бюджетних коштів, отриманих за надання платних послуг, якщо таким закладам законом надано відповідне право; надходження, що отримують державні і комунальні заклади фахової перед вищої та вищої освіти, наукові установи та заклади культури як відсотки, нараховані на залишок коштів на поточних рахунках, відкритих у банках державного сектору для розміщення власних надходжень, отриманих як плата за послуги, що надаються ними згідно з основною діяльністю, благодійні внески та гранти.

Власні надходження бюджетних установ використовуються (з урахуванням частини дев'ятої статті 51 цього Кодексу) на:
– покриття витрат, пов'язаних з організацією та наданням послуг, що надаються бюджетними установами згідно з їх основною діяльністю (за рахунок надходжень підгрупи 1 першої групи);
– організацію додаткової (господарської) діяльності бюджетних установ (за рахунок надходжень підгрупи 2 першої групи);
– утримання, облаштування, ремонт та придбання майна бюджетних установ (за рахунок надходжень підгрупи 3 першої групи);
– ремонт, модернізацію чи придбання нових необоротних активів та матеріальних цінностей, покриття витрат, пов'язаних з організацією збирання і транспортування відходів і брухту на приймальні пункти (за рахунок надходжень підгрупи 4 першої групи);
– господарські потреби бюджетних установ, включаючи оплату комунальних послуг і енергоносіїв (за рахунок надходжень підгруп 2 і 4 першої групи);
– організацію основної діяльності бюджетних установ (за рахунок надходжень підгруп 1 та 3 другої групи);
– виконання відповідних цільових заходів (за рахунок надходжень підгрупи 2 другої групи).

Враховуючи вищезазначене та з урахуванням постанови Кабінету Міністрів України від 30.03.2011 № 314 «Про умови оплати праці працівників державних спеціалізованих установ судових експертиз» необхідно зробити розрахунок вартості нормо години при наданні різного роду послуг, визначених законодавством.

Науково-дослідним центром судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України розробляється Методика визначення вартості нормо години під час проведення судових експертиз та надання платних послуг науково-дослідними установами судових експертиз Міністерства юстиції з метою можливості використання її у експертній практиці при проведенні експертних досліджень та наданні платних послуг.

Список використаних джерел:

1. Бюджетний кодекс України: Кодекс України від 08.07.2010 р. № 2456-VI: станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2456–17#Text (дата звернення: 19.06.2024).

2. Деякі питання надання платних послуг науково-дослідними установами судових експертиз Міністерства юстиції: Постанова Каб. Міністрів України від 27.07.2011 р. № 804: станом на 9 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/804–2011-п#Text (дата звернення: 19.06.2024).

3. Про судову експертизу: Закон України від 25.02.1994 р. № 4038-XII: станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/4038–12#Text (дата звернення: 19.06.2024).

ДО ПИТАННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА НЕЗАКОННЕ ПЕРЕПРАВЛЕННЯ ОСІБ ЧЕРЕЗ ДЕРЖАВНИЙ КОРДОН УКРАЇНИ

Євген ТЕРЛЕЦЬКИЙ
аспірант наукової лабораторії
з проблем протидії злочинності
Навчально-наукового інституту № 1
Національної академії внутрішніх справ

Демократизація державних інституцій неможлива без наступальної боротьби зі злочинністю у різних її проявах. Держава в особі компетентних органів визначає правила поведінки, що спрямовані на гарантування безпеки кожній особі, а також встановлення стану захищеності суспільства та держави від різного роду протиправних посягань на охоронювані інтереси. Порушення цих приписів може призвести до завдання непоправної шкоди ефективній діяльності держави у різних її сферах [10, с. 389]. У зв'язку із зростанням суспільної небезпеки перед державою постає питання щодо забезпечення ефективної охорони як окремого громадянина, так і всього суспільства в цілому [5, с. 5]. Системна перебудова правоохоронних органів України, створення нових правозастосовних підрозділів, удосконалення існуючих нормативно-правових актів у сфері боротьби з організованою злочинністю, у тому числі транснаціональною, вкотре підтвердила, що така боротьба є глобальною проблемою, яку неможливо вирішити на рівні окремої держави, правоохоронного органу чи нормативно-правового акту [9, с. 110]. Саме тому протидія злочинності у багатьох країнах світу відіграє вирішальну роль при формуванні безпекової політики у різних сферах державного управління [6, с. 33–47; 7, с. 31–39; 8, с. 60–64].

З огляду зазначене проблема незаконного переправлення осіб через державний кордон України сьогодні залишається складною та актуальною. Протидія діяльності організаторів нелегальної міграції – одна з проблем, вирішенням яких займаються уповноважені органи, а боротьба з нелегальною міграцією вважається одним із головних завдань Державної прикордонної служби України та Служби безпеки України [16, с. 168].

Так, наприклад у першому півріччі 2024 року контррозвідники СБУ заблокували канал нелегальної міграції іноземців через Україну до країн ЄС. За попередніми даними, протиправним механізмом скористалося понад 100 осіб.

Як встановила СБУ, організаторами схеми були мешканці Києва та їх іноземні спільники. Вони створили механізм протиправного перебування в Україні вихідців з країн Південної Азії.

Зловмисники створили низку фіктивних фірм та за програмою міжнародного студентського обміну, оформлювали фіктивні запрошення іноземцям нібито на навчання до українських вишів.

Але замість навчання, на підставі отриманих запрошень, «студенти» мали можливість виїздити до країн ЄС, використовуючи Україну як перевальний пункт.

За даними слідства, учасники групи діяли по всій території України. Вони зустрічали мігрантів, забезпечували житлом та попередньо «легалізовували» в Україні під фіктивними документами. У подальшому ділки формували групи та переправляли «студентів» за кордон.

За попередніми оцінками, зловмисники переправили каналом нелегальної міграції понад 100 іноземців. Вартість «послуг» залежала від країни призначення та коливалася від 4 до 8 тис. доларів США. Найбільшим «попитом» серед мігрантів користувалися країни Західної Європи.

У рамках кримінального провадження одному з організаторів повідомлено про підозру за ч. 2 ст. 332 (незаконне переправлення осіб через державний кордон України) КК України [14].

Також на Волині працівники ДБР викрили злочинну групу, яка переправляла військовозобов'язаних через кордон до Польщі.

Допомагала зловмисникам інспекторка одного з прикордонних загонів на Волині.

Клієнтів ділки шукали у соцмережах, а вартість послуг складала 3,5 тис. доларів США з особи.

З ними заздалегідь домовлялись про зустріч і доправляли автомобілем до пункту пропуску. Водій-спільник передавав прикордонниці закордонні паспорти пасажирів. Інспекторка не вносила відомості про них до автоматизованої системи обміну інформацією щодо контролю осіб, які перетинають державний кордон. Це давало можливість чоловікам перетнути кордон і потрапити до Польщі.

За даними слідства, за такою схемою група переправила за межі держави понад 168 осіб.

Інспекторці повідомлено про підозру у незаконному переправленні осіб через державний кордон України за попередньою змовою групою осіб, з використанням свого службового становища (ч. 2 ст. 332 КК України) [1].

Необхідно також зазначити, що з урахуванням широкомасштабної воєнної агресії РФ проти України характер злочинів пов'язаних з порушенням державного кордону зазнав певних змін. Це зумовлено як соціально-економічними змінами у суспільстві, так і спрямованістю політики держави на розвиток і розширення контактів з іншими країнами. Наслідки таких перетворень є, безумовно, позитивними, проте часто використовуються злочинними елементами (збільшення контрабанди, наркобізнес, торгівля людьми, зброєю, нелегальна міграція тощо). Незаконне переправлення осіб через державний кордон може здійснюватись як на в'їзд, так і на виїзд. Останніми десятиліттями географічне положення України почали активно використовувати з метою нелегальної міграції, транспортування мігрантів та торгівлі людьми. Водночас Україна відіграє важливу роль у стримуванні потоків нелегальної міграції зі Сходу до держав Центральної та Західної Європи [4; 13, с. 4].

Аналіз показників злочинності в Україні за останні роки свідчить, що частка злочинів, учинених іноземцями та особами без громадянства, щорічно у загальному масиві зареєстрованих кримінальних правопорушень сягає близько 1%. Виходячи з офіційних статистичних даних, не можна з упевненістю стверджувати, що злочинні діяння іноземців та осіб без громадянства не становлять значної загрози для українського суспільства, адже злочинам, що вчиняються цими категоріями осіб, властива латентність. До того ж в умовах політичної та міжнародної ситуації, в якій опинилася Україна останніми роками, кримінологічна характеристика цього сегменту злочинності стає гострою та актуальною [3, с. 8].

За інформацією Державної прикордонної служби України, які збігаються з даними прикордонних служб країн Європи, дають значно менші цифри. У кінці 2023 року було зафіксовано 22,9 млн. виїздів з України з початку великої війни та понад 20,1 млн. в'їздів [18]. Різниця становила близько 2,81 млн. осіб, тоді як наведена вище оцінка кількості українських мігрантів від УВКБ ООН значно її перевищує. Можна припустити, що тимчасовий прихисток отримала значна частина українців, які виїхали до лютого 2024 року з інших, переважно економічних причин [17].

Водночас, залежно від розвитку воєнно-політичної обстановки в країні у 2024 році існує велика ймовірність збільшення міграційних процесів з України [19].

За інформацією уповноваженого Верховної Ради України з прав людини, з 24 лютого 2022 року із України виїхало понад 14,5 млн. громадян, із них як мінімум 11,7 млн. осіб – до країн Євросоюзу [11], серед яких багато жінок та дітей, людей з інвалідністю, дітей-сиріт та дітей, що позбавлені батьківського піклування, людей похилого віку, стали потенційними жертвами злочинів, пов'язаних з торгівлею людьми. Наведені категорії осіб є вразливими не лише у фізичному, але й у ментальному плані, адже переживають стрес зі значними негативними наслідками, що позначається на їх ментальному здоров'ї, підвищуючи вразливість.

Аналіз звітності ДМС України за 2023 рік дає підстави стверджувати, що сьогодні залишають країну переважно люди працездатного віку, що негативно впливає на внутрішній ринок праці, і у найближчій перспективі держава почне відчувати нестачу працездатного населення [2]. Особливо дана проблема відчувається при високому рівні еміграції висококваліфікованих кадрів, таких як вчені, програмісти, лікарі та ін. В такому випадку, може спостерігатися дефіцит трудових ресурсів і відбуватися зниження продуктивності праці в країнах походження [15, с. 62].

Україна є країною – донором робочої сили для держав ЄС. Лише незначна частина трудових мігрантів стають легальними трудовими мігрантами в країнах-реципієнтах. Більшість з них займається незареєстрованою діяльністю, тобто є нелегальними трудовими мігрантами. Окрема частина українських мігрантів є жертвами злочинних угруповань, що займаються торгівлею людьми, і зайнята протиправною діяльністю не з власної волі [12].

Сферу контролю за міграцією та ефективного прикордонного менеджменту Європейська Комісія та уряд України визнали пріоритетною у відносинах України та ЄС. Динаміка розвитку відносин між Україною та ЄС у сфері полегшення людських контактів, відкриття спільного кордону для вільного руху осіб залежатиме від здатності України контролювати власні кордони і протидіяти явищам нелегальної міграції, торгівлі людьми, контрабанди, міжнародної організованої злочинності [12].

Як бачимо, проблеми кримінальної відповідальність за незаконне переправлення осіб через державний кордон України були і залишаються актуальними для правозастосовних органів. Особливої уваги це питання набуло під час широкомасштабного вторгнення та розв'язання збройної агресії РФ на території України.

Враховуючи викладене, з метою попередження та відвернення більш тяжких наслідків до яких може призвести незаконне переміщення осіб через державний кордон України в умовах воєнного стану чи в особливий період, пропонуються зміни та доповнення до ст. 332 КК України. У зв'язку з чим вбачається за доцільне доповнити ст. 332 КК України частиною четвертою, яка буде мати таку законодавчу конструкцію:

«4. Дії, передбачені частиною першою, другою або третьою цієї статті, вчинені в умовах воєнного стану чи в особливий період,–

караються позбавленням волі на строк від восьми до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років з конфіскацією майна.».

Список використаних джерел:

1. ДБР викрило на Волині злочинну групу, яка незаконно переправила через кордон майже 170 осіб. https://dbr.gov.ua/news/dbr-vikrilo-na-volini-zlochinnu-grupu-yaka-nezakonno-perepravila-cherez-kordon-majzhe-170-osib (дата звернення: 15.06.2024).

2. Звіт Голови ДМС України за результатами роботи у 2023 році. URL: https://dmsu.gov.ua/news/dms/15875.html (дата звернення: 15.06.2024).

3. Калініна А.В. Злочинність іноземців та осіб без громадянства в Україні: кримінологічна характеристика і стратегія запобігання: монографія [за заг. ред. В.В. Голіна]. Харків. Право. 2019. 304 с.

4. Кузьменко О.В. Основні проблеми нелегальної міграції на Україні. URL: http://inter.criminology.onua.edu.ua/?p=1269 (дата звернення: 16.06.2024).

5. Луценко Ю.В. Звільнення від кримінальної відповідальності за злочини проти основ національної безпеки України. Харків. Право. 2015. 200 с.

6. Луценко Ю.В. Поняття та зміст воєнної безпеки України у світлі сучасних викликів та загроз. Актуальні проблеми міжнародних відносин. Випуск 137. 2018. С. 33–47.

7. Луценко Ю.В. Поняття, система та класифікація видів безпеки в контексті міжнародного правопорядку. Соціально-правові студії. 2019. Випуск 4 (6). С. 31–39.

8. Луценко Ю.В. Протидія злочинності у світлі міжнародного правопорядку. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2023. Том 34 (73) № 5. С. 60–64.

9. Луценко Ю.В. Участь спеціальних служб іноземних держав у протидії організованій злочинності та корупції на прикладі Італійської Республіки. Наше право. 2017. № 4. С. 110–116.

10. Луценко Ю.В., Тарасюк А.В. Актуальні проблеми удосконалення окремих положень кримінального та кримінального процесуального законодавства України. Юридичний науковий електронний журнал. 2023. № 1. С. 388–391.

11. Омбудсмен розповів, скільки українців виїхало за кордон із 24 лютого. URL: https://www.slovoidilo.ua/2022/12/01/novyna/polityka/ombudsmen-rozpoviv-skilky-ukrayincziv-vyyixalo-kordon-24-lyutoho (дата звернення: 15.06.2024).

12. Політика України у сфері контролю над нелегальною міграцією. URL: https://www.icps.com.ua/assets/uploads/images/images/eu/migration_policy_ukr.pdf (дата звернення: 15.06.2024).

13. Розслідування незаконного переправлення осіб через державний кордон України: метод. рек. / [Чернявський С.С., Вознюк А.А., Брисковська О.М. та ін.]. К.: Нац. акад. внутр. справ, 2017. 64 с.

14. СБУ заблокувала потужний канал нелегальної міграції в ЄС через Україну. URL: https://ssu.gov.ua/novyny/sbu-zablokuvalapotuzhnyi-kanal-nelehalnoi-mihratsii-v-yes-cherez-ukrainu (дата звернення: 18.06.2024).

15. Цевух Ю.О. Вплив міжнародної трудової міграції на національний ринок праці. Емпіричні підходи щодо вивчення рівня добробуту у країнах СНД; зб. наук. праць міжнар. наук.–практ. семінару; ОНУ ім. І.І. Мечникова. Одеса, 2012. С. 61–63.

16. Шульга А.М., Цвіркун Н.Ю. Підстави кримінальної відповідальності за незаконне переправлення осіб через державний кордон України. Вісник кримінологічної асоціації України. 2017. № 1(15), С. 167–177.

17. Як інші країни після воєн повертали своїх мігрантів і що робити Україні. URL: https://www.epravda.com.ua/columns/2024/05/2/713185/ (дата звернення: 15.06.2024).

18. Яка демографічна ситуація в Україні: дані соціології. URL: https://www.pravda.com.ua/columns/2023/09/23/7421114/ (дата звернення: 15.06.2024).

19. Ukraine Refugee Situation. URL: https://data.unhcr.org/en/situations/ukraine#_ga=2.92194970.188031801.1670859078–711474979.1670859078 (дата звернення: 15.06.2024).

СТАТУС УЧАСНИКІВ ПРИВАТНИХ ВІЙСЬКОВИХ ТА ОХОРОННИХ КОМПАНІЙ В МІЖНАРОДНОМУ ГУМАНІТАРНОМУ ПРАВІ ТА ШЛЯХИ ІМПЛЕМЕНТАЦІЇ НОРМ ДО НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА

Антон ТИМОФЄЄВ
старший викладач
Національного юридичного
університету імені Ярослава Мудрого

У зв'язку з постійним розвитком світу та все більшою глобалізацією, не рідким стають не тільки численні процедури обміну товарів між країнами, але й численні збройні конфлікти, які можуть мати своєю ціллю захоплення ресурсів або територій. При цьому, відповідно до ч. 4 ст. 2 Статуту ООН, усі Члени Організації Об'єднаних Націй утримуються в своїх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і якимось іншим чином, несумісним із Цілями Об'єднаних Націй [1]. Саме у зв'язку з цим, для досягнення своїх цілей, досить таки часто державами залучаються приватні військові та охоронні компанії (далі – ПВОК), які можуть виконувати дуже різний спектр обов'язків в рамках збройних конфліктів. Розгалуженість робіт та послуг, які можуть надаватись представниками ПВОК, виникає чимало питань в контексті їхнього статусу в рамках збройного конфлікту.

На сьогоднішній день регулювання ПВОК на міжнародному рівні є недостатнім. Найбільш комплексним документом, в якому описана регуляція їх діяльності, є Документ Монтрьо, який не має загальнообов'язкового статусу, а лише рекомендаційний. При цьому, самі по собі ПВОК поділяються на такі види залежно від функцій:

- компанії бойового забезпечення (combat provider companies), які надають своїм клієнтам послуги з підтримання бойових дій їхніх сил безпеки й оборони (за термінологією НАТО – тактичну підтримку), включно з безпосередньою участю в бойових операціях.
- воєнні консалтингові компанії (military consulting companies), які спеціалізуються на наданні послуг із планування, створення, реформування й розвитку сил безпеки й оборони, зокрема органів розвідки та контррозвідки, їхньої бойової та спеціальної підготовки тощо.
- воєнні логістичні компанії (military logistic companies), діяльність яких охоплює: обслуговування й експлуатацію складних систем озброєння, військової техніки та комп'ютерних систем, матеріально-технічне забезпечення військ, будівництво військових об'єктів [2].

Саме від специфіки виконання певних функцій і буде залежати їхній статус в рамках збройного конфлікту, зокрема в контексті взяття особи в полон.

Відповідно до ст. 4 (А) Третьої Женевської конвенції встановлено ряд категорій осіб, які отримують статус військовополоненого при їх потраплянні в полон. Вищевказані категорії ПВОК можна співставити з положеннями Конвенції наступним чином:

- особи, які залучені в роботі компаній бойового забезпечення, зокрема ті, які безпосередньо беруть участь у збройних конфліктах є військовополоненими відповідно до ст. 4 (А) (1) Третьої Женевської конвенції, як особовий склад збройних сил сторони конфлікту, а також члени ополчення або добровольчих загонів, які є частиною цих збройних сил;
- особи, які залучені до діяльності воєнних логістичних та консалтингових компаній є військовополоненими відповідно до ст. 4 (А) (4) Третьої Женевської конвенції, як особи, які супроводжують збройні сили, але фактично не входять до їхнього складу [3].

Така позиція підтверджується також і Документом Монтрьо. Згідно з п. 26 якого, персонал ПВОК:

– зобов'язаний, незалежно від свого статусу, дотримуватися чинного міжнародного гуманітарного права;
– перебуває під захистом міжнародного гуманітарного права як цивільні особи, якщо тільки вони не включені до складу регулярних збройних сил держави до складу регулярних збройних сил держави або є членами організованих збройних сил, груп або підрозділів під командуванням, відповідальним перед державою або іншим чином втрачають свій захист, як це визначено міжнародним гуманітарним правом;
– має право на статус військовополоненого в міжнародному збройному конфлікті, якщо вони є особами які супроводжують збройні сили, що відповідає вимогам статті 4 (A) (4) Третьої Женевської конвенції [4].

У зв'язку з повномасштабною агресією росії по відношенню до України, у нашій країні гостро постало питання регулювання діяльності ПВОК, які в подальшому могли б якісно перебрати на себе певні завдання, що на сьогоднішній день покладені на сектор безпеки та оборони. На зараз у Верховній Раді України зареєстровано законопроект № 11214 від 26.04.2024, який передбачає регулювання міжнародних оборонних компаній. Проте в даному законопроекті не врегульовано питання членів ПВОК в контексті міжнародного гуманітарного права, що може призвести до юридичної невизначеності у майбутньому [5].

Підводячи підсумок, слід зазначити, що важливою є точна і своєчасна імплементація норм міжнародного гуманітарного права в національне законодавство задля уникнення майбутніх правових колізій у цій сфері.

Список використаних джерел:

1. Статут Організації об'єднаних націй: Міжнародний договір від 26.06.1945 р. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf (дата звернення: 20.06.2024).

2. Кохан Г.Л. Правові питання діяльності приватних військових компаній: міжнародний аспект. *Вчені записки*, 2020. С. 190–201. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_3/33.pdf (дата звернення: 20.06.2024).

3. Женевська конвенція про поводження з військовополоненими: Міжнародний договір від 12.08.1949 р. URL: https://zakon.rada.gov.ua/laws/show/995_153#n196 (дата звернення: 20.06.2024).

4. Документ Монтрьо від 02.10.2008 р. URL: https://www.icrc.org/en/download/file/135841/montreux_document_en.pdf (дата звернення: 20.06.2024).

5. Проект Закону про міжнародні оборонні компанії: Законопроект від 26.06.2024 р. № 11214. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/44120 (дата звернення: 20.06.2024).

ОСНОВНІ ГАРАНТІЇ ДЕРЖАВИ ЩОДО ЗАХИСТУ ПРАВ ЖІНОК ПІД ЧАС ЗБРОЙНОГО КОНФЛІКТУ

Юрій ТКАЧЕНКО
кандидат економічних наук, доцент,
завідувач відділу післядипломної освіти
Національного наукового центру
«Інститут судових експертиз» ім. Засл. проф. М.С. Бокаріуса

Одним із негативних проявів війни (збройного конфлікту) є соціальну нерівність у суспільстві, зокрема, посилення вразливості маргіналізованих груп у порівнянні з мирним часом. Дослідження свідчать про те, що жінки страждають від наслідків війни (збройних конфліктів) непропорційно більше, ніж чоловіки, і становлять значну частку цивільного населення, яке

страждає від війни. Міжнародне гуманітарне право намагається створити рамки для обмеження шкоди від збройного конфлікту для всіх, хто не бере або вже не бере участі у бойових діях. Під час війни міжнародне гуманітарне право надає жінкам загальний захист як цивільним особам, а також спеціальний захист, який враховує, що жінки можуть бути особливо вразливими до конкретних видів насильства.

Як відомо, жінки становлять найбільшу частку біженців або вразливих осіб, які евакуюються разом з дітьми та людьми похилого віку. Віддаленість чоловіків від сім'ї та тривала участь у збройних конфліктах призводить до того, що соціальний статус жінок також змінюється. Жінка бере на себе всю відповідальність із догляду за дітьми та людьми похилого віку, стаючи головним охоронцем сім'ї, гарантом безпеки та ідентичності.

Водночас зауважуємо, що стосується захисту жінок під час збройних конфліктів, то важливо розглянути відповідні правові інструменти, які створюють основу для захисту жінок під час війни (збройного конфлікту), а також способи їх інституціоналізації.

Так, чотири Женевські конвенції 1949 року та два Додаткові протоколи 1977 року встановлюють систему рівного ставлення, в якій не може бути дискримінації цивільних осіб, ув'язнених, переміщених осіб, осіб з особливими потребами, поранених, хворих, осіб, які зазнали корабельної аварії, або осіб, які підлягають покаранню. Дискримінація за ознакою статі допустима лише тоді, коли очікується, що її наслідки будуть сприятливими. Такий підхід до рівності санкціонує норми, що забезпечують спеціальний захист жінок відповідно до Женевської конвенції та Додаткових протоколів до неї.

Система спеціальних положень для жінок ґрунтується на поняттях, які вимагають особливої поваги та захисту жінок. Женевська конвенція I, стаття 12 (4) та Женевська конвенція II, стаття 12 (4) стверджують, що «до жінок слід ставитися з усією повагою, яка відповідає їхній статі», Додатковий протокол I, стаття 76 (1) стверджує, що «жінки є об'єктом особливої поваги і підлягають захисту, зокрема, від зґвалтування, примусу до проституції та будь-яких інших непристойних посягань», а Женевська конвенція III, стаття 88 (3) стверджує, що «У жодному випадку жінок-військовополонених не засуджують до більш суворого покарання і не застосовують до них більш суворого режиму під час відбуття покарання, ніж режим, що його застосовують у випадку покарання за аналогічні правопорушення чоловіків зі складу збройних сил держави, що тримає в полоні.». Самі по собі слова «особлива повага», «повага» і «міркування, зумовлені їхньою статтю» просто формують принципову заяву, форму прохання, а не конкретне зобов'язання. Вони доповнюються дещо чіткішими правилами для конкретних цілей.

Крім того зазначаємо, що особливо беззахисними перед негативними наслідками збройного конфлікту реально першочергово стають жінки-матері неповнолітніх дітей та вагітні жінки. Дуже часто сам стан вагітності чи наявність дитини використовується учасниками збройного конфлікту як засіб шантажу, погрози для примусу жінки вчинити певні небажані для неї дії. Серед міжнародного законодавства, що спрямоване на підтримку таких жінок можна відзначити Четверту Женевську Конвенцію, яка передбачає, що вагітні жінки та матері малолітніх дітей повинні одержувати додаткове харчування згідно з їх фізіологічними потребами. Матерів малолітніх дітей повинні приймати в будь-якій установі, здатній забезпечити їх належне лікування та медичну допомогу, рівноцінну тій, що отримує населення.

Жінки як військовополонені належать до вразливої категорії жертв війни та збройних конфліктів, та їх наслідків. Однак, досвід війни в Україні показує, що росія не дотримується даної Конвенції щодо жінок-військовополонених, що викликає серйозне занепокоєння міжнародного співтовариства.

В українському законодавстві норми про поводження саме з жінками-військовополоненими в період збройних конфліктів знаходяться на стадії розробки. Звичайно слід брати до уваги особливість категорії полонених. Тому є підстави для постановки питання про розробку, наприклад, правил обміну саме жінок як полонянок або звільнення воюючими сторонами, з огляду на обставини їх здоров'я, як у документі міжнародного, так і національного характеру.

Кримінально-виконавчим кодексом України та Кримінальним процесуальним кодексом України передбачено конкретні механізми захисту жінок і сімей в мирний час. Проте ці положення не були призначені для застосування під час конфлікту. Однак, такі положення залишаються актуальними, оскільки вони можуть бути застосовані з метою імплементації міжнародного гуманітарного права, а також бути інформативним джерелом рекомендацій щодо належного підходу.

Разом з тим зазначаємо, що ідеальний підхід до змін передбачає розробку комплексних методів моніторингу виконання Україною норм міжнародного гуманітарного права. Важливим заходом для покращення моніторингу є присутність жінок під час збору та інтерпретації даних. Це необхідно, оскільки документуванням досвіду жінок у конфліктах часто займаються чоловіки, які не враховують важливі порушення прав жінок, окрім насильства. Окрім того, працівники компетентних правоохоронних органів та органів прокуратури не завжди ознайомлені з принципами та стандартами роботи з постраждалими від таких злочинів. Саме тому, видається необхідним, щоб відповідні органи влади України забезпечували систематичний збір інформації щодо випадків вчинення актів насильства, пов'язаного із конфліктом, зокрема, з метою передачі до Канцелярії прокурора Міжнародного кримінального суду.

Проблема захисту прав жінок в умовах воєнних конфліктів є складною та багатогранною, вимагаючи чітких міжнародних законодавчих актів, здатних до практичного втілення з конкретними рішеннями. Хоча законодавство України щодо захисту жінок під час збройних конфліктів є досить розвиненим, існують труднощі з його дотриманням сторонами конфлікту через невизначеності, що супроводжують такі конфлікти. Додатковою проблемою, яка потребує міжнародної уваги, є питання участі жінок у воєнних діях. Особливої уваги заслуговує захист жінок-військовополонених з урахуванням їхнього становища.

Враховуючи вищевикладене, можна констатувати, що жінки є достатньо вразливою соціальною ланкою громадянського суспільства у період війни (збройного конфлікту). Жінки, окрім виховання дітей та догляду за людьми похилого віку є повноправними учасниками опору воєнній агресії, а саме: волонтерами; активними членами суспільства; правозахисниками; комбатантами; тощо. Вони також є учасниками усіх суспільних процесів, які виникають під час війни (збройного конфлікту). Окрім вищезгаданого з'явилась нагальна необхідність додатково вивчати проблематику жінки-волонтера у частині правового захисту, за умови, коли вони потрапляє до полону, а саме до якої категорії військово полонених їх можна відносити (військовополонені чи цивільні). Як показує практика, незважаючи на наявний прогрес у розвитку правової бази щодо дотримання і гарантування прав жінок – питання їх захисту під час збройних конфліктів і надалі залишається актуальною проблемою сьогодення. Україна, міжнародні органи та організації повинні спрямовувати свої зусилля на ефективну імплементацію існуючих правових документів та вжиття заходів щодо покращення стану жінок, а також попередження злочинів й захисту жінок не тільки у мирний час, а й у період війни (збройного конфлікту) від будь-яких злочинів шляхом забезпечення ефективного правового захисту.

Список використаних джерел:

1. Луцан А.В. Захист прав жінок в умовах збройних конфліктів. Право і суспільство. 2022. № 6. С. 299–306. URL: https://doi.org/10.32842/2078–3736/2022.6.45 (дата звернення: 17.06.2024).

2. Джуган В.О. Проблеми захисту прав жінок під час воєнних дій в україні. Юридичний науковий електронний журнал. 2022. № 9. С. 146–148. URL: https://doi.org/10.32782/2524–0374/2022–9/34 (дата звернення: 14.06.2024).

3. Громовенко К.В. Особливості захисту прав людини в умовах збройних конфліктів. Правові новели. 2022. № 17. С. 101–107. URL: https://doi.org/10.32847/ln.2022.17.14 (дата звернення: 14.06.2024).

МОРСЬКА ВІЙНА ТА ЗАХИСТ МОРСЬКИХ ЗОН ВІДПОВІДНО ДО МГП: ОЦІНКА ПОЛОЖЕНЬ МГП У СУЧАСНИХ МОРСЬКИХ КОНФЛІКТАХ

Василь ТРОНЦ
співробітник СБУ
Степан БОНДАРЕНКО
співробітник СБУ

Світовий океан є життєво важливим для глобальної торгівлі, транспорту та видобутку ресурсів. Війна на морі порушує цю діяльність і може мати руйнівні наслідки для цивільного населення та морського середовища. Міжнародне гуманітарне право (МГП) відіграє вирішальну роль в обмеженні цих негативних наслідків, регулюючи ведення військових дій на морі та забезпечуючи захист цивільного населення та невійськових об'єктів. Війна на морі має довгу та складну історію, яка з'явилася ще до письмових законів. Проте нормативно-правова база, яка його регулює, з часом значно змінилася. Хоча звичаєве право існувало століттями, кодифіковані норми з'явилися в 19 і 20 століттях через такі договори, як Гаазька конвенція (1907) і Друга Женевська конвенція (1949). Ці документи встановлюють принципи МГП, що застосовуються до морської війни, зокрема розрізнення між військовими та цивільними об'єктами, пропорційність нападів та захист персоналу, який зазнав корабельної аварії.

Морська війна була важливим аспектом військової стратегії та конфлікту з давніх часів. З появою сучасних технологій і міжнародної правової бази проведення військово-морських операцій стало предметом складних правил міжнародного гуманітарного права (МГП). Захист морських зон, включаючи територіальні води, виключні економічні зони (ВЕЗ) і міжнародні води, залишається критичним питанням для національної безпеки, економічної стабільності та глобального миру. Розуміння правових параметрів, що регулюють морські дії та захист морських зон відповідно до МГП, має важливе значення для забезпечення дотримання міжнародних норм, запобігання незаконним діям на морі та захисту людського життя та майна під час збройних конфліктів.

Міжнародне гуманітарне право, також відоме як право збройних конфліктів, спрямоване на обмеження наслідків збройних конфліктів з гуманітарних причин. Воно захищає тих, хто не бере участь у бойових діях, і обмежує засоби і методи ведення війни. У морському контексті положення МГП мають вирішальне значення для регулювання морської війни, враховуючи унікальні характеристики та складність морських операцій. Правові рамки, що регулюють морську війну, походять з різних джерел, включаючи Женевські конвенції, Конвенцію ООН з морського права (UNCLOS) і звичаєве міжнародне право. У цьому дослідженні нами розглядаються певні тонкощі морської війни згідно з МГП, зосереджуючись на захисті морських зон. Також нами розглядаються відповідні законодавчі положення, виклики в їх реалізації та взаємодія між інтересами національної безпеки та міжнародно-правовими зобов'язаннями.

Регулювання військово-морської війни значно змінилося протягом століть, відображаючи зміни у морській техніці, стратегії та міжнародних відносинах. Ранні морські закони, такі як Consolato del Mare (14 ст.) і Паризька декларація (1856 р.), заклали основу для сучасних правил військово-морської війни [1; 2, с. 179]. Гаазькі конвенції 1899 і 1907 років додатково кодифікували правила ведення морської війни, вирішуючи такі питання, як поводження з моряками, які потерпіли аварію, і встановлення нейтральних зон.

Наслідки Другої світової війни та подальше створення Організації Об'єднаних Націй призвели до значного прогресу в регулюванні військово-морських дій. Женевські конвенції 1949 року та Додаткові протоколи до них 1977 та 2005 років запровадили комплексний захист для жертв збройних конфліктів, у тому числі на морі [3]. Прийняття UNCLOS у 1982 році за-

безпечило детальну правову основу для використання океанів і морів, встановлюючи права та обов'язки для морських держав і вирішуючи такі питання, як територіальні води, виключні економічні зони та відкрите море.

МГП зобов'язує сторони конфлікту розрізняти комбатантів і некомбатантів, а також між військовими та цивільними об'єктами. У морському контексті цей принцип вимагає, щоб напади були спрямовані лише на законні військові цілі, уникаючи цивільних суден та інфраструктури. Принцип пропорційності забороняє напади, які можуть спричинити випадкову втрату життя серед цивільного населення, поранення цивільних осіб або пошкодження цивільних об'єктів, що було б надмірним по відношенню до конкретної та очікуваної прямої військової переваги. Командувачі військово-морських сил повинні ретельно розглянути можливі супутні збитки своїх операцій.

Фундаментальний принцип розрізнення забороняє напади на цивільних осіб і цивільні об'єкти. У морському контексті необхідно розрізняти військові кораблі, військові допоміжні судна та торгові судна. Військові кораблі є законними військовими цілями, тоді як торговельні судна, як правило, користуються імунітетом від нападу, якщо вони не беруть активної участі у бойових діях.

Принцип пропорційності встановлює, що атаки мають бути спрямовані на військові цілі, а очікувана шкода цивільному населенню має бути пропорційною очікуваній військовій перевазі. Цей принцип стає особливо складним у морській війні через потенціал широкого побічного збитку від нападів на кораблі або використання певної зброї, наприклад морських мін. Принцип необхідності регламентує, що сила має застосовуватися лише в тій мірі, в якій це вимагається військовими цілями конфлікту. Цей принцип обмежує застосування надмірної сили, яка спричиняє непотрібні страждання.

Військові кораблі вважаються законними військовими цілями і можуть бути атаковані без попередження. Проте МГП захищає персонал, який зазнав корабельної аварії, якого необхідно рятувати та поводитися з ними гуманно. Торговельні кораблі зазвичай користуються імунітетом від нападу. Однак вони можуть втратити цей імунітет за певних обставин, наприклад, якщо: 1) беруть безпосередню участь у бойових діях (наприклад, мають зброю чи війська); наявна спроба чинити опір законному захопленню (наприклад, втікаючи після чіткого попередження зупинитися); 3) використовуються для забезпечення блокади. Блокади є законними засобами ведення війни, метою яких є запобігання постачанню ворога. Однак вони повинні бути оголошені, ефективними та неупереджено застосовуватися до всіх держав. Блокади також мають забезпечити пропуск гуманітарної допомоги. Морські зони відчуження обмежують доступ до певної морської території, часто з міркувань безпеки. Хоча в МГП це прямо не зазначено, їх законність залежить від їх мети та від того, чи відповідають вони принципам МГП, зокрема принципу розрізнення та свободи судноплавства. Використання автономної зброї у морській війні викликає значне занепокоєння щодо дотримання принципів МГП, зокрема вимоги щодо людського судження під час прийняття рішень щодо цілей.

Застосування МГП у морській війні представляє унікальні виклики: 1) обмежена рамка договору – порівняно з сухопутною війною норми МГП для військово-морської війни є менш кодифікованими, значною мірою покладаються на звичаєве право та тлумачення; 2) технологічний прогрес – нові технології, такі як автономна зброя та кібервійна, створюють нові проблеми для тлумачення та застосування принципів МГП; 3) складність розслідування: розслідування передбачуваних порушень на морі може бути складним через величезні океани та суперечки щодо юрисдикції.

Постійно мінливий ландшафт морських конфліктів вимагає критичної оцінки адекватності положень міжнародного гуманітарного права (МГП). Сьогоднішня морська війна характеризується технологічним прогресом, стиранням меж між учасниками бойових дій і цивільним населенням і появою недержавних акторів. Що стосується відповідних міжнародно-правових норм, то ми виділяємо наступні: 1) Гаазька конвенція V (1907) – обмежує використання торпед у морській війні, забороняє установку невибіркових мін; 2) Гаазька конвенція IX (1907) – керує

бомбардуванням військово-морських сил у воєнний час, потрібне попередження перед нападом на незахищені міста, села, житла чи будівлі; 3) Женевська конвенція II (1949) – захищає поранених, хворих і потерпілих корабельну аварію членів збройних сил на морі, вимагає від сторін конфлікту шукати, збирати та евакуювати постраждалих без розрізнення національності чи воюючих сторін; 4) IV Женевська конвенція (1949) – захищає цивільне населення та цивільні об'єкти у воєнний час, у тому числі на морі, забороняє невибіркові атаки та вимагає всіх можливих запобіжних заходів для мінімізації шкоди цивільному населенню; 5) Додатковий протокол I до Женевських конвенцій (1977) – ще раз підтверджує та зміцнює принципи МГП, що застосовуються до міжнародних збройних конфліктів, визначає цивільних осіб і цивільні об'єкти та пропонує додатковий захист для них.

Незважаючи на сильні сторони МГП, існує низка слабкостей, на які варто звертати увагу. Нові технології, такі як автономна зброя та кібервійна, створюють проблеми в тлумаченні та застосуванні принципів МГП. МГП насамперед регулює поведінку держави під час збройних конфліктів. Зростаюча роль недержавних акторів, таких як пірати та терористичні групи, потребує подальших правових рамок. Законність МЗВ зон, які часто використовуються для обмеження доступу до певних морських районів, прямо не розглядається в МГП. Їх законність залежить від їх мети та дотримання принципів МГП. Контроль за порушеннями МГП на морі є складним через просторі океани та суперечки щодо юрисдикції. Проблемою залишається розслідування інцидентів та притягнення порушників до відповідальності.

Морські конфлікти продовжують формувати сучасні міжнародні відносини, оскільки країни змагаються за контроль над стратегічними водними шляхами, природними ресурсами та територіальними претензіями. Суперечка щодо Південно-Китайського моря передбачає збіг територіальних претензій між Китаєм, В'єтнамом, Філіппінами, Малайзією, Брунеєм і Тайванем [4]. Великі претензії Китаю, засновані на історичних твердженнях і «лінії з дев'ятьма рисками», призвели до напруженості та конфронтації з сусідніми державами. До порушень міжнародно-правових норм належать: будівництво Китаєм штучних островів і військових об'єктів у спірних водах порушує виключні економічні зони (ВЕЗ) і морські права сусідніх держав, порушуючи Конвенцію ООН з морського права (UNCLOS) [5]. Рішення Постійної палати третейського суду (PCA) 2016 року, яке визнало недійсним позов Китаю про «дев'ять пунктирів», підкреслило нехтування Китаєм міжнародними правовими нормами та його відмову виконувати рішення трибуналу [6].

Суперечка щодо Східно-Китайського моря обертається навколо «суперечливих» претензій між Китаєм і Японією щодо островів Сенкаку/Дяоюйдаою [7]. Обидві країни стверджують суверенітет над островами, які розташовані на багатих рибальських угіддях і потенційних запасах нафти та газу. До порушень міжнародно-правових норм належать: порушення UNCLOS – одностороннє оголошення Китаєм зони розпізнавання протиповітряної оборони (ПВО) над Східно-Китайським морем і її вторгнення в японські територіальні води порушує положення UNCLOS щодо свободи судноплавства та польотів. Інциденти з морським патрулюванням, протистояння берегової охорони та військові позиції як Китаю, так і Японії посилили напругу в регіоні, викликаючи занепокоєння щодо ризику збройного конфлікту.

Суперечка щодо Фолклендських/Мальвінських островів включає суперечливі претензії між Аргентиною та Сполученим Королівством щодо суверенітету в Південній Атлантиці [8]. Виявлення запасів нафти і газу в регіоні знову розпалило напруженість між двома країнами. До порушень міжнародно-правових норм належать: порушення UNCLOS: спроби Аргентини обмежити морський доступ до Фолклендських/Мальвінських островів порушують морські права жителів Фолклендських островів і суперечать положенням UNCLOS щодо свободи судноплавства та доступу до ресурсів. Незважаючи на спроби вирішити суперечку дипломатичними засобами, включаючи переговори та арбітраж під егідою ООН, Аргентина та Великобританія не змогли досягти взаємоприйнятного рішення, що продовжило конфлікт.

Незважаючи на ці виклики, МГП залишається життєво важливою основою для регулювання війни на морі та захисту цивільного населення та морського середовища. Постійні зусилля

держав, міжнародних організацій і вчених-юристів мають вирішальне значення для адаптації та зміцнення МГП для вирішення сучасних морських загроз і технологічного прогресу. На завершення це дослідження підкреслює важливість детального розуміння правових та етичних аспектів військово-морської війни в рамках МГП. З'ясовуючи права, обов'язки та проблеми, з якими стикаються воюючі сторони, що діють у морських зонах, це дослідження сприяє зусиллям, спрямованим на посилення захисту цивільних осіб, мінімізацію шкоди навколишньому середовищу та дотримання гуманітарних принципів у морських конфліктах. Він наголошує на важливості продовження діалогу, співпраці та дотримання міжнародних правових норм для вирішення складних викликів військово-морської війни в сучасному геополітичному ландшафті. Підсумовуючи, сучасні морські конфлікти створюють значні виклики для міжнародного миру, безпеки та співпраці. Спричинені геополітичним суперництвом, територіальними суперечками, конкуренцією за ресурси та проблемами безпеки, ці конфлікти мають далекосяжні наслідки для регіональної стабільності, економічного процвітання та екологічної стійкості. Ефективне управління та вирішення морських конфліктів вимагають дотримання міжнародних правових норм і рамок, включаючи UNCLOS, юриспруденцію Міжнародного суду та механізми вирішення спорів. Багатостороннє співробітництво, діалог і заходи зміцнення довіри є важливими для пом'якшення напруженості, сприяння безпеці на морі та захисту прав та інтересів усіх учасників морського транспорту у все більш взаємопов'язаному та взаємозалежному світі.

Список використаних джерел:

1. Home – Consolato del Mare Ltd. URL: https://www.shippinglawyers.eu/ (дата звернення: 13.06.2024).

2. Малишко В.М. Паризька декларація про морські війни 1856 року та скасування каперства. Науковий вісник Національної академії внутрішніх справ. № 1. 2014. С. 177–188.

3. Конвенція про захист цивільного населення під час війни: Конвенція; ООН від 12.08.1949 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/995_154 (дата звернення: 13.06.2024)

4. Territorial Disputes in the South China Sea | Global Conflict Tracker. Global Conflict Tracker. URL: https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea (дата звернення: 13.06.2024).

5. UNCLOS: United Nations Convention on the Law of the Sea. URL: https://www.unclos.org/ (дата звернення: 13.06.2024).

6. Tribunal Issues Landmark Ruling in South China Sea Arbitration. Default. URL: https://www.lawfaremedia.org/article/tribunal-issues-landmark-ruling-south-china-sea-arbitration (дата звернення: 13.06.2024).

7. Chapman Bert. «Geopolitical implications of the Sino-Japanese East China Sea dispute for the U.S.» Geopolitics, History, and International Relations, vol. 9, no. 2, 2017, pp. 15–54. JSTOR, https://www.jstor.org/stable/26806119 (дата звернення: 13.06.2024).

8. A Short History of the Falklands Conflict. Imperial War Museums. URL: https://www.iwm.org.uk/history/a-short-history-of-the-falklands-conflict#:~: text=The%20Falklands%20Conflict%20was%20a, and%20cost%20over%20900%20lives. (дата звернення: 13.06.2024).

РОЗВИТОК СУЧАСНИХ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ: ШЛЯХ ДЛЯ ОПТИМІЗАЦІЇ ПРАВОВИХ ПРОЦЕСІВ ТА ПЕРСПЕКТИВНІ НАПРЯМКИ ІМПЛЕМЕНТАЦІЇ МІЖНАРОДНИХ ПРАВОВИХ СТАНДАРТІВ В НАЦІОНАЛЬНУ ПРАВОВУ СИСТЕМУ

Олександр ЧЕРЕДНИЧЕНКО
кандидат економічних наук, доцент,
професор Національного юридичного
університету імені Ярослава Мудрого

Кінець XX-го століття надав поштовх до стрімкого розвитку інноваційних технологій основою для яких виступило розповсюдження та широке використання можливостей всесвітньої мережі Інтернет, цифрових технологій, гаджетів та IT-технологій. Завдяки революційним досягненням у техніці та науці наприкінці минулого та початку XXI століття можна стверджувати, що суспільство перейшло від індустріального до інформаційного стану. Це, в свою чергу, викликало необхідність розробки систем збереження та використання накопичених інформаційних ресурсів, наукових досліджень, технологій, знань, правил та норм тощо.

В умовах постійних впроваджень і вдосконалень правова система теж не залишалася осторонь. Фахівці різних технологічних галузей намагалися модернізувати та удосконалити правничу сферу, адже вона є не тільки запорукою демократії та справедливості в державі, а й базою для ведення господарської діяльності у всіх сферах господарювання, договореної та нормотворчої роботи. Доречи, саме цей перехід є дуже важливим для правової сфери, адже тепер людство отримало невичерпний ресурс доступу до інформації та можливість отримати юридичні послуги «не виходячи з дому», протягом нетривалого часу та без довготривалих затримок.

Саме розвиток сучасних технологій відкриває нові шляхи для оптимізації правових процесів, доступності правової допомоги. Як слідство, автоматизація (діджиталізація) правової системи безпосередньо впливає на швидкість вирішення справ, зменшення бюрократії, мінімізацію помилок та співпрацю між юридичними партнерами, правоохоронними органами і судовою системою.

До впровадження широкого використання сучасних інформаційних технологій і можливостей діджиталізації правники здійснювали ручну обробку та аналіз правової інформації, самостійно шукаючи, оглядаючи паперові документи, закони, судові прецеденти та ін. При цьому залучалися всі наявні джерела (насамперед першоджерела): друковані книги із законами, кодексами, іншими нормативно-правовими документами, судові рішення, постанови, інструкція та правила тощо. Створювалися і використовувалися безліч картотек, які виконували роль сучасних автоматизованих баз даних. Також, на державному рівні не існувало можливості синхронізації бази даних юридичних осіб (підприємств, установ, закладів, ін.) та громадян (фізичних осіб), єдиних доступних автоматизованих систем судових рішень, виконавчих проваджень і їх результатів. Існували відомчі бази даних (МВС, органів держ.безпеки, прикордонної служби та митних органів, експертно-криміналістичних центрів, нотаріату та інших відомств), але доступ до більшості із них був обмежений із-за причин наявності інформації з обмеженим доступом, недостатнім та недосконалим програмним забезпеченням та забезпеченням електронно-обчислювальної техніки, відсутністю онлайн-платформ, а також з причин відомчих обмежень щодо обміну інформацією. Пошук і отримання необхідної інформації, наприклад, правового характеру займав безліч часу та людських ресурсів, не виключав похибку при зборі та використанні даних, потребував від виконавця пильності при обробці інформації

та підвищував ризик помилок, різко обмежував доступ до джерел із-за їх обмеженої кількості та друкованого формату зберігання, ускладнював доступ до міжнародних правових актів. Як результат, неоптимальне використання ресурсів призводило до обробки правником значних масивів інформації, в тому числі такої яка безпосередньо не потрібна для тої чи іншої справи, а це призводило до затягування рішень у часі. Обмеженість технологій доступу до правової інформації вимагала залучення всіх можливих засобів, але не вирішувало вищенаведених проблем.

В теперішній час ситуація кардинально відрізняється від минулого. Вже створено та активно використовується багато цифрових застосунків, що надає можливість у вільному доступі до джерел, які полегшують справу правників.

Найпоширеніший із них у нашій країні – офіційний сайт Верховної Ради України, zakon.rada.gov.ua, де правники у вільному доступі можуть знайти всі текстові версії нормативно-правових актів нашої держави**,** які не мають грифу обмеження [10]. Юристам більше не потрібно шукати закони загального доступу в архівах, юридичних бібліотеках та довідкових матеріалах. Це набагато спрощує опрацювання документів, зменшує часові витрати.

Схожим сайтом є ips.ligazakon.net, який теж має інформацію про законодавство України, але його відмінність полягає в тому, що він має ширшу базу правової інформації, таку як авторські права, інтелектуальна власність, а також він має такий додаток, як калькулятор штрафів.

Зі світових цифрових юридичних застосунків можна виділити Casetext, Westlaw тощо.

Casetext – це юридичний онлайн-інструмент, який використовує штучний інтелект для аналізу законодавства, пошуку судових рішень, він надає доступ до широкого спектру юридичних джерел [2].

Westlaw – одна із найбільших юридичних баз даних для багатьох країн світу. Вона містить міжнародні юридичні матеріали, повну базу прецедентного права, публікації видатних спеціалістів у різних галузях права та багато іншої корисної інформації для правників. Westlaw, об'єднує більше ніж 40 тис. баз даних, та HeinOnline, особливістю якої є представлення документів тільки у вигляді PDF-файлів, відсканованих з першоджерел [9].

Документи міжнародного та міждержавного рівня оцифровано та викладено на офіційних сайтах міжнародних організацій, таких як:

Організація Об'єднаних Націй – електронні версії рішень Генеральної Асамблеї, декларацій, конвенцій, резолюцій тощо.

Європейський Союз – резолюції, постанови, регламенти, директиви ЄС тощо.

Рада Європи – стратегії, конвенції, меморандуми, плани дій Ради тощо.

Таким чином, проблема вільного, швидкого доступу до джерел інформації (насамперед до нормативно-правових актів як національного так і міжнародного характеру) було вирішено саме завдяки впровадженню новітніх інформаційних технологій.

Наступним вагомим вкладом людства в розвиток юриспруденції стало запровадження системи електронного судочинства. Було створено Єдиний державний реєстр судових рішень України та електронну платформу: «Електронний суд» (ЄСІТС) [11]. Вона забезпечує можливість подання позовної заяви в онлайн-режимі, обміну документами між учасниками судового процесу та судом, формування електронних ордерів для правників, але найголовнішою інновацією є проведення судового засідання в режимі відео-конференції.

Схожою електронною платформою є судова система США «Public Acces to Court Electronic Records» [7]. Дана система забезпечує публічний доступ до положень федеральних судів за відповідну оплату (0,1 доларів США за сторінку документа; 2,4 долари США за аудіо-файл), надає можливість електронної подачі документів.

Як результат, судам стало значно легше працювати, маючи єдині електронні бази даних своєї установи на заміну паперовій документації. Це сприяє ефективності та швидкості розгляду справ, а також підвищення довірі з боку клієнтів.

Досить складною була співпраця між юридичними партнерами: щоб вирішити спільні справи, питання, потрібна була фізична присутність усіх членів обговорення, на що не завжди

є час і можливість. Наразі людство винайшло рішення і цієї проблеми, а саме було створено онлайн-платформи, відео-конференції, які дозволяють спілкуватися, обмінюватися інформацією та документами всім членам бесіди без географічної присутності. Обмін документів, їх підпис в онлайн-режимі можливий завдяки електронним системам документообігу.

Для проведення конференцій зазвичай використовують такі онлайн-платформи, як Google Meet, Microsoft Teams, Zoom. Вони багатофункціональні, мають інструменти забезпечення конфіденційності, а також дозволяють проводити конференції як для декількох людей, так і для великого колективу.

Застосунками для юридичної співпраці є Netdocuments, MyCase та ін.

Netdocuments – це хмарна система управління документами, однією з її спеціалізацій є сумісна співпраця над документацією. Платформа забезпечує надійний захист даних, адже має справу з важливою інформацією [6].

MyCase – програмне забезпечення, що надає можливість керувати справами, спілкуватися з клієнтами, ставити електронний підпис тощо [5].

Для юриспруденції важлива довіра громадян, бо вся їх робота побудована навколо суспільства. У цьому правникам деяким чином допомагають електронні системи публічних закупівель. Ця новинка, окрім покращення стосунків із людьми, сприяє автоматизованості системи закупівель та ефективному спостереженню за ними, зменшенню корупційних ризиків.

Прикладом таких платформ є Funding & Tenders, Prozorro, Contracts Finder тощо.

F&T – європейська централізована платформа, яка спеціалізується на тендерах та контрактах країн Європейського Союзу і має спрощену систему пошуку за ключовими словами [3].

Prozorro – наша, українська, платформа публічних закупівель, де кожен громадянин може побачити всю тендерну документацію держави, очікувану вартість та учасників тендеру[1].

Contracts Finder – англійська електронна платформа, на якій доступні контракти й тендери державних закупівель на суми, що перевищують дванадцять тисяч фунтів стерлінгів [4].

В останній час збільшується використання можливостей штучного інтелекту, в тому числі з боку фахівців-правників. Так, ще декілька років тому важко було уявити собі що роботи будуть можуть бути «працівниками суду» або «аналітиками чи оперативниками правоохоронної сфери». Штучний інтелект дійсно допомагає в аналізі даних, швидкому пошуку інформації. Він набагато полегшує роботу правникам у сфері юстиції, але все ж таки не можна повністю довіряти інтернет-машині, адже правові рішення це не суперечки на вулиці, а реальні проблеми, які потрібно вирішити ефективно та якісно, і тому вся інформація, яку юристам надає інтелектуальний агент, повинна ретельно відфільтровуватися. Зараз доречно поки що використовувати таку допомогу як допоміжну. Доречи, цей формат є гарним допоміжним заходом для моделювання ситуацій, операцій, можливих шляхів розвитку оперативної обстановки, шляхів прийняття рішень, можливих дій злочинців тощо. Впевнений, що з таким прогресом у науково-технічній сфері не можна виключати можливість, що штучний інтелект стане надійним помічником судочинства та правоохоронної системи.

Актуальність даної тематики визначається тим, що нашу епоху можна охарактеризувати як «інноваційну» стадію розвитку суспільства, усіх сфер людського буття. Правознавство, і як з точки зори соціальної науки, і як прикладна сфера, є однією із найперших галузей, де повинні впроваджуватися різноманітні технології, застосовуватися сучасні підходи для вдосконалення юридичної системи. І дуже важливим є те, щоб громадяни, а тим паче правники, розумілися в різних аспектах новинок. Громадяни повинні мати уявлення щодо системи права хоча б на «масовому» рівні, а правникам же важливо розвивати інформаційну культуру, щоб бути професіоналами у своїй діяльності.

Список використаних джерел:

1. Про нас | ProZorro. Головна | Prozorro. URL: https://prozorro.gov.ua/about (дата звернення: 10.06.2024);

2. Casetext Online Legal Research Service Review. Lawyerist. URL: https://lawyerist.com/reviews/online-legal-research/casetext (дата звернення: 10.06.2024);

3. EC's new Funding & Tender Opportunities Portal is online | Ideal-ist. Ideal-ist. URL: https://www.ideal-ist.eu/news/ecs-new-funding-tender-opportunities-portal-online (дата звернення: 10.06.2024);

4. Government Digital Service. Contracts Finder. GOV.UK. URL: https://www.gov.uk/contracts-finder (дата звернення: 13.01.2024);

5. Legal Case Management Software and Solutions | MyCase. MyCase. URL: https://www.mycase.com (дата звернення: 10.06.2024);

6. Legal Document Management for Lawyers and Law Firms – NetDocuments. NetDocuments – Document and Email Management for Legal Firms and Departments. URL: https://www.netdocuments.com/solutions/industries/law-firms (дата звернення: 10.06.2024);

7. PACER Pricing: How fees work | PACER: Federal Court Records. Public Access to Court Electronic Records | PACER: Federal Court Records. URL: https://pacer.uscourts.gov/pacer-pricing-how-fees-work (дата: звернення 10.06.2024);

8. Place of performance (Map) – TED Tenders Electronic Daily. Place of performance (Map) – TED Tenders Electronic Daily. URL: https://ted.europa.eu/TED/browse/browseByMap.do (дата звернення: 10.06.2024);

9. Westlaw International – Our Solutions. Westlaw International. URL: https://www.westlawinternational.com/our-solutions (дата звернення: 10.06.2024);

10. Верховна Рада України. URL: https:.www.rada.gov.ua/ (дата звернення: 10.06.2024);

11. Єдиний державний реєстр судових рішень. URL: https:.reyestr.court.gov.ua/ (дата звернення: 10.06.2024).

ЩОДО ІМПЛЕМЕНТАЦІЇ НОРМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА ПРО СТАТУС ВІЙСЬКОВОПОЛОНЕНОГО ДО КПК УКРАЇНИ

Микола ЧЛЕНОВ
старший викладач
Національного юридичного
університету імені Ярослава Мудрого

Після початку широкомасштабної збройної агресії рф проти України, науковці та практики в сфері кримінальної юстиції стали активніше вивчати положення міжнародного гуманітарного права (далі – МГП), які спрямовані на забезпечення дотримання прав людини в період збройних конфліктів, а також пом'якшення наслідків цих конфліктів, спираючись на принципи гуманного ставлення до людини. На території України представники окупаційних військ держави-агресора щоденно вчиняють величезну кількість злочинів, зокрема проти миру та безпеки людства. Введений в Україні воєнний стан, обстановка ведення воєнний дій, наявність великої кількості потерпілих (жертв) від наслідків збройного конфлікту, викликають необхідність слідчим, прокурорам, суддям переосмислити раніше вживані поняття «терористи», «бойовики» та глибше вивчити та розуміти зміст таких понять МГП як «комбатант», «військовополонений», «найманець», «законна воєнна ціль» тощо.

Україна вживає заходів щодо суворого дотримання норм МГП, передбачених Женевською конвенцією про поводження з військовополоненими від 12.08.1949, Додатковим протоколом до ЖК (Протокол I) від 08.06.1977 шляхом імплементації до національного законодавства та удосконалення діючих норм щодо правового статусу військовополонених, забезпечення правил утримання, поводження із військовополоненими, що перебувають у полоні під владою України.

Під «військовим полоном» розуміється обмеження свободи осіб, які безпосередньо брали участь зі зброєю в руках у бойових діях проти супротивника, головною метою військового полону є припинення участі цієї категорії осіб у бойових діях.

Військовополонені – особи, які мають право на цей статус відповідно до ст. 4 Женевської конвенції про поводження з військовополоненими від 12.08.1949 р. (далі – ЖК (ІІІ)) та ст. 44 Додаткового протоколу І до ЖК (ІІІ) від 12 серпня 1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол І), від 8 червня 1977 р.[1].

Військовополоненими є особи, які потрапили в полон до супротивника й на-лежать до однієї з таких категорій:

1) особовий склад збройних сил сторони конфлікту, а також члени ополчення або добровольчих загонів, які є частиною цих збройних сил;

2) члени інших ополчень та добровольчих загонів, зокрема члени організованих рухів опору, які належать до однієї зі сторін конфлікту й діють на своїй території або за її межами, навіть якщо цю територію окуповано, за умови, що ці ополчення або добровольчі загони, зокрема організовані рухи опору, відповідають таким умовам: а) ними командує особа, яка відповідає за своїх підлеглих; б) вони мають постійний відмітний знак, добре розпізнаваний на відстані; в) вони носять зброю відкрито; г) вони здійснюють свої операції згідно із законами та звичаями війни;

3) члени особового складу регулярних збройних сил, які заявляють про свою відданість урядові або владі, що не визнані державою, яка їх затримує;

4) особи, які супроводжують збройні сили, але фактично не входять до їх-нього складу, наприклад цивільні особи з екіпажів військових літаків, військові кореспонденти, постачальники, особовий склад робочих підрозділів або служб побутового обслуговування збройних сил за умови, що вони отримали на це дозвіл тих збройних сил, які вони супроводжують, для чого останні видають їм посвідчення особи;

5) члени екіпажів суден торговельного флоту, зокрема капітани, лоцмани та юнги, а також екіпажів цивільних повітряних суден сторін конфлікту, які не користуються більш сприятливим режимом згідно з будь-якими іншими положеннями міжнародного права;

6) жителі неокупованої території, які під час наближення ворога озброюються, щоб чинити опір силам загарбника, не маючи часу сформуватися в регулярні війська, за умови, що вони носять зброю відкрито й дотримуються законів і звичаїв війни [2].

За останні два роки законодавець прийняв ряд нормативно-правових актів для щодо врегулювання питань поводження з військовополоненими, зокрема:

– постанову КМУ від 05.04.2022 № 413 «Про затвердження Порядку тримання військовополонених»;
– постанову КМУ від 11.03.2022 № 257 «Про утворення Координаційного штабу з питань поводження з військовополоненими»;
– постанову КМУ від 17.06.2022 № 721 «Про затвердження Порядку здійснення заходів щодо поводження з військовополоненими в особливий період» та інші.

Крім того, на підставі Закону України № 2472-IX від 28.07.2022 до КПК України внесено наступні зміни, які спрямовані на подолання труднощів розслідування в умовах воєнного стану, а також імплементацію в кримінальний процес окремих норм МГП, зокрема щодо статусу військовополонених, які стосуються:

– появи нового суб'єкта – «особу, стосовно якої уповноваженим органом прийнято рішення про обмін як військовополоненого», якою є будь-яка особа, яка має процесуальний статус підозрюваного, обвинуваченого, засудженого та яка включена відповідним уповноваженим органом до списку для обміну як військовополонений (п. 28 ст. 3 КПК);
– підстави скасування запобіжного заходу – у зв'язку з прийняттям уповноваженим органом рішення про передачу підозрюваного, обвинуваченого для проведення обміну як військовополоненого (ст. 201–1 КПК);
– розширення суб'єктів для здійснення слідчим суддею допиту під час досудового розслідування, а саме: особи, стосовно якої уповноваженим органом прийнято рішення про

обмін як військовополоненого та закріплення цих показань як доказів (абз. 2 ч. 1 ст. 225 КПК України);

- підстави зупинення спеціального досудового розслідування – якщо уповноваженим органом прийнято рішення про передачу підозрюваного для обміну як військовополоненого та підозрюваним надано письмову згоду на проведення такого обміну (п. 5 ч. 1 ст. 280 КПК), а також відновлення спеціального досудового розслідування коли обмін підозрюваного як військовополоненого проведено або такий обмін не відбувся (ст. 282 КПК);
- підстави для здійснення спеціального досудового розслідування (in absentia) – розслідування злочину, вчиненого підозрюваним, стосовно якого уповноваженим органом 1) прийнято рішення про передачу його для обміну як військовополоненого та 2) такий обмін відбувся (абз. 2 ч. 2 ст. 297–1 КПК);
- підстави для здійснення спеціального судового розгляду за відсутності обвинуваченого (in absentia) – якщо стосовно нього уповноваженим органом прийнято рішення про передачу його для обміну як військовополоненого та такий обмін відбувся (абз. 2 ч. 3 ст. 323 КПК);
- підстави зупинення судового провадження, якщо уповноваженим органом прийнято рішення про передачу обвинуваченого для обміну як військовополоненого та обвинуваченим надано письмову згоду на такий обміну (ч. 2 ст. 335 КПК),
- підстави звільнення від відбування покарання у зв'язку з прийняттям рішення про передачу особи для обміну як військовополоненого (п. 13–4 ст. 537 КПК) [3].

Пам'ятка про права і обов'язки підозрюваного – це процесуальний документ, що містить узагальнену інформацію про права та обов'язки підозрюваного під час кримінального провадження і вручається, згідно з ч. 8 ст. 42 КПК України, одночасно з повідомленням про підозру особою, яка здійснює таке повідомлення у випадках і на підставах, передбачених ст. 276 КПК України. Уповноваженими суб'єктами на вручення Пам'ятки є слідчий, детектив, прокурор, уповноважена службова особа, яка має право здійснювати затримання та відповідальна за перебування затриманих осіб у підрозділі органу досудового розслідування. Пам'ятка містить права підозрюваного, передбачені КПК України та іншими нормативно-правовими актами, які відображають мету її вручення – повідомлення і роз'яснення підозрюваному його прав та обов'язків, що є основою дотримання його процесуальних прав.

Чинний КПК України не містить вимог до змісту вказаної пам'ятки. На практиці, до неї включають витяги положень Конституції України (ст. 28, 29, 55, 56, 59, 62, 63), ЗУ «Про попереднє ув'язнення» (ст. 9, 10), КПК України (ст. 42, 52, 54, 285, 268, 269, 472, 473).

На нашу думку, Пам'ятка про процесуальні права та обов'язки підозрюваного, який також має статус військовополоненого, має відрізнятись від звичайної пам'ятки підозрюваного за рахунок доповнення її наступними положеннями:

- право на подання письмової заяви про згоду на його обмін на полоненого захисника України, що знаходиться у військовому полоні держави-агресора (ст. 220–1 КПК);
- право приймати участь у судовому засіданні з розгляду слідчим суддею клопотання прокурора про скасування запобіжного заходу у зв'язку з прийняттям уповноваженим органом рішення про передачу підозрюваного для обміну як військовополоненого та заявляти заяви та клопотання з цього приводу (ст. 201–1 КПК);
- про обов'язок начальника установи попереднього ув'язнення звільнити з-під варти особу, стосовно якої уповноваженим органом прийнято рішення про обмін як військовополоненого, у день отримання ухвали слідчого судді, суду про скасування запобіжного заходу. В такому випадку військовополонений передається під нагляд представникам уповноваженого органу, що відповідає за поводження з військовополоненими, для організації та проведення її обміну як військовополоненого (ч. 10 ст. 20 ЗУ «Про попереднє ув'язнення»);
- положення Частини II «Загальні положення про захист військовополонених» (ст. 12–16) Женевської конвенції про поводження з військовополоненими від 12.08.1949.

Крім того, в національному законодавстві мають бути врегульовані порядок, строки та суб'єкти, уповноважені повідомити державу, громадянином якої є підозрюваний/обвину-

вачений з числа військовополонених про факт його знаходження у військовому полоні, про адресу місця тримання.

Висновок: Відношення до військовополонених є індикатором дотримання гуманітарних принципів і міжнародного гуманітарного права. В КПК України процесуальний статус та права підозрюваного, який є військовополоненим, знаходяться на етапі становлення та підлягають законодавчому удосконаленню з метою врегулювання строків та порядку взаємодії органів слідства, прокуратури та суду з уповноваженим органом – Координаційним центром з питань поводження з військопополоненими, визначення переліку прав і обов'язків підозрюваного, який є військовополоненим. Ці законодавчі зміни сприятимуть удосконаленню правового регулювання питань поводження з військовополоненими, які мають статус підозрюваного/обвинуваченого у кримінальному провадженні та запобіганню порушенню їх процесуальних прав. Запропоновані законодавчі зміни стануть важливим кроком у зміцненні процесуального статусу військовополоненого у кримінальному провадженні.

Список використаних джерел:

1. Про затвердження порядку тримання військовополонених: постанова КМУ від 05.04.2022 № 413. URL: https://zakon.rada.gov.ua/laws/show/413–2022-%D0%BF#n23 (дата звернення: 20.06.2024).

2. Інструкція про порядок виконання норм міжнародного гуманітарного права у Збройних Силах України: наказ Міністерства оборони України від 23.03.2017 № 164. URL: https://zakon.rada.gov.ua/laws/show/z0704–17#Text (дата звернення: 20.06.2024).

3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text (дата звернення: 20.06.2024).

4. Женевська конвенція про поводження з військовополоненими від 12.08.1949. URL: https://zakon.rada.gov.ua/laws/show/995_153#Text (дата звернення: 20.06.2024).

МІСЦЕ І РОЛЬ ВІЙСЬКОВОЇ ЕКСПЕРТИЗИ ЩОДО ДОСЛІДЖЕННЯ НАСЛІДКІВ ДІЙ (БЕЗДІЯЛЬНОСТІ), ПРИЙНЯТИХ УПРАВЛІНСЬКИХ РІШЕНЬ ВІЙСЬКОВИМИ СЛУЖБОВИМИ (ПОСАДОВИМИ) ОСОБАМИ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ ТА ЗБРОЙНИХ СИЛ УКРАЇНИ ПІД ЧАС ЗБРОЙНОЇ АГРЕСІЇ (ЗБРОЙНОГО КОНФЛІКТУ) В УМОВАХ ВОЄННОГО СТАНУ

Сергій ШЕРЕМЕТОВ
судовий експерт
Київського відділення Національного
наукового центру «Інститут судових
експертиз ім. Засл. проф. М.С. Бокаріуса»

Війна, збройна агресія (збройний конфлікт), під час якої гине та отримує фізичні і моральні каліцтва мирне населення, руйнуються матеріальні цінності, створені народом країни, яка потерпає від агресора, по суті є злочином проти людства, миру і безпеки життя.

Існування численних ганебних явищ, пов'язаних із збройними конфліктами, у 21 сторіччі свідчіть про слабку систему безпеки в світі. Можна стверджувати про відсутність її дієвої ефективності.

Провідні держави світу та міжнародні організації виявилися неспроможними ефективно протистояти таким глобальним викликам XXI століття, як поглиблення нерівномірності розвитку, активізація тероризму та інших видів незаконної діяльності міжнародних злочинних угруповань, боротьба за природні ресурси та проблеми надійності їх транспортування, ризик неконтрольованого розповсюдження зброї масового ураження, триваючі та «заморожені» конфлікти. Для України проблема захисту життєво важливих національних інтересів залишається надзвичайно складною. За 17 років незалежності українській владі, нажаль, не вдалося досягти суттєвих успіхів у формуванні та реалізації ефективної політики національної безпеки. Кризові явища, притаманні майже всім сферам внутрішнього життя країни та зовнішніх відносин, виразно демонструють відсутність довгострокової стратегії та стратегічного менеджменту в діяльності влади [1].

Головними зовнішніми викликами (загрозами) для національної безпеки України, є наступні:

– послаблення дієвості міжнародного права, побудованого на застарілих принципах міжнародних інститутів, та відповідно – зменшення зовнішніх гарантій безпеки України;
– загострення ситуації в зонах «заморожених» конфліктів;
– посилення розбіжностей на євроатлантичному просторі на тлі зростання конфронтації Росії і країн Заходу та, як наслідок,– збільшення ризику перетворення України на буферну зону;
– наявність глобальних ризиків і загроз, таких, як тероризм, розповсюдження ЗМУ, нелегальна міграція тощо.

Актуальність зовнішніх викликів посилюється наявністю внутрішніх проблем, які набули загрозливого характеру:

– гостра міжпартійна конфронтація, неспроможність поступитися політичними амбіціями, політична боротьба «на знищення» з використанням спекуляцій на питаннях безпеки, надмірного популізму, поступове зростання розриву між так званою політичною елітою і суспільством;
– критичне розшарування суспільства за регіональними, політичними, майновими, релігійними, мовними ознаками;
– неефективність державного апарату, брак стратегічного державного підходу до планування стратегічного розвитку країни і суспільства, організації взаємодії залучених галузей і органів виконавчої влади, посадових осіб, мотивації та контроль організації з метою досягнення координації людських, фінансових, природних і технологічних ресурсів, необхідних для ефективного виконання завдань (менеджменту);
– слабкість демократичних інститутів, залежність судової системи від політичних впливів і як наслідок – неспроможність держави забезпечити належний рівень дотримання прав і свобод громадян;
– розбалансованість системи національної безпеки через неузгодженість реформ у різних структурах сектору безпеки, послаблення можливостей реагування на кризові явища, зростання протиріч між змістом і темпами реформування Збройних Сил, інших структур сектору безпеки, з одного боку, і процесом наближення України до членства в НАТО – з іншого;
– критичний стан озброєння та військової техніки, низький рівень забезпечення та бойової підготовки Збройних Сил [1].

Нажаль Україна 24.02.2022 стикнулась саме з таким явищем – збройною агресію.

Відповідно до своїх обов'язків, визначених Конституцією України, Президент України, Верховний Головнокомандувач України Указом від 24.02.2022 № 64/2022 «Про введення воєнного стану в Україні», затвердженого Законом України № 2102-IX від 24.02.2022, ввів режим воєнного стану [2].

Воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень [3].

При відсічи агресії найважливішу роль відіграє обороноздатність держави. Обороноздатність держави – здатність держави до захисту у разі збройної агресії або збройного конфлікту. Вона складається з матеріальних і духовних елементів та є сукупністю воєнного, економічного, соціального та морально-політичного потенціалу у сфері оборони та належних умов для його реалізації [3].

Оборона України – система політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту [3].

Вона базується на готовності та здатності органів державної влади, усіх складових сектору безпеки і оборони України, органів місцевого самоврядування, єдиної державної системи цивільного захисту, національної економіки до переведення, при необхідності, з мирного на воєнний стан та відсічі збройній агресії, ліквідації збройного конфлікту, а також готовності населення і території держави до оборони [3]. Тобто, у відсічі збройної агресії повинні і приймають участь всі галузі національної економіки та верстви населення, які можуть по статусу та за станом здоров'я і зобов'язані приймати активну участь у відсічі збройній агресії.

Відповідно до статті 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [3]. Забезпечення державної безпеки і захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом. Збройні Сили України та інші військові формування ніким не можуть бути використані для обмеження прав і свобод громадян або з метою повалення конституційного ладу, усунення органів влади чи перешкоджання їх діяльності.

Згідно зі статтею 17 Конституції України на Збройні Сили України покладаються оборона України, захист її суверенітету, територіальної цілісності і недоторканності [4].

Існує помилкова думка, що першими на збройну агресію іншої держави повинні реагувати Збройні Сили країни.

Збройній агресії передують:

– вивчення воєнно-політичної обстановки в світі, країні, на яку готується напад, суміжних країнах;
– вивчення настрою, лояльності (або негативного відношення) політичного керівництва, населення держави, на яку готується напад;
– прораховуються можливі варіанти розвитку подій за різними сценаріями;
– створюються коаліції, визначаються потенційні і залучаються до підготовки дійсні спільники майбутнього вторгнення;
– активно проводяться зустрічі з лідерами інших країн і в прихованій формі дізнаються про ставлення до майбутніх бойових дій;
– за допомогою ЗМІ готується суспільство різних країн щодо доцільності і виправдовування агресії з використанням неправдивої інформації (створення заборонених міжнародною спільнотою зразків озброєння (біологічних, хімічних, радіоактивних, варварських), гуманітарна катастрофа (раптові масові вбивства мирного населення, авторитарні деспотичні режими, утиснення прав нацменшин);

– готується суспільна думка населення країни-агресора щодо необхідності вторгнення;
– готуються до великого навантаження національна економіка, промисловий і науковий потенціал, населення країни;
– готуються збройні сили до вторгнення;
– активно ведеться розвідувальна і агентурна робота.

Цей перелік підготовчих дій до агресії можна продовжувати. З цього слідує, що першими, другими і наступними повинні реагувати насамперед дипломатичні, розвідувальні, законодавчі органи.

Збройні Сили, безумовно, повинні реагувати і бути готові до відсічі нападу, але реагування ЗС – це похідна від дій вищевказаних органів, які повинні зробити все можливе для запобігання або своєчасного повідомлення (попередження) про збройну агресію іншої держави.

Збройна агресія (збройний конфлікт) висуває до військових службових (посадових) осіб МОУ та ЗСУ вимоги не тільки широких знань військового мистецтва на найвищому рівні, але і знання на такому ж і навіть більш вищому рівні знань міжнародного гуманітарного права, звичаїв ведення війни, законодавства, інших нормативно-правових актів щодо отримання, обліку і використання озброєння та військової техніки (ОВТ), боєприпасів, матеріальних засобів (МЗ) благодійної (волонтерської) допомоги, трофейного ОВТ, боєприпасів і МЗ.

З початком ведення бойових дій з метою відсічі Україною збройної агресії раптово зріс негативний показник чисельних правопорушень з боку військових службових (посадових) осіб за ознаками кримінальних правопорушень, передбачених КК України, які вчиняються при виконанні службових (посадових) обов'язків. До цього переліку можна віднести: незаконне заволодіння представниками силових структур матеріальними засобами громадян України; незаконне проникнення в житлові приміщення; незаконне застосування стрілецької та іншої зброї відносно цивільного населення, що призвело до великої кількості смертельних випадків; незаконне застосування стрілецької зброї, яке спричинило загибель та поранення цивільного населення на блок-постах; незаконне нарахування та отримання грошової винагороди за участь у бойових діях; незаконне отримання благодійної (волонтерської) допомоги; залишення зброї, ОВТ, боєприпасів, МЗ в місцях ведення бойових дій; прийняті управлінські рішення, які призвели до втрат зброї, ОВТ, боєприпасів, МЗ; привласнення військовими службовими (посадовими) особами, у тому числі високопосадовцями, грошових коштів у великих розмірах; закупівля майна і продуктів харчування за явно завищеними цінами з порушенням процедур закупівель тощо.

Деякі злочини, особливо у фінансово-господарській галузі, військовими службовими (посадовими) особами МОУ та ЗСУ набули широкого розголосу, що викликає у населення України обурення, розчарування та недовіру до влади і, як наслідок, пошук можливостей уникнути конституційного обов'язку захищати свою Батьківщину.

Тому проведення судових військових експертиз за спеціальністю 16.1 «Військові дослідження» безспірно займає важливе місце в боротьбі правоохоронних органів з військовою злочинністю.

До 2015 року військові експертизи науково-дослідними установами судових експертиз Міністерства юстиції України не проводилися. Зазначений вид експертизи був запроваджений наказом Міністерства юстиції України від 27.07.2015 № 1350/5.

Предметом судової військової експертизи є встановлення судовим військовим експертом фактів (суджень про факти) по визначених слідчим або судом питаннях щодо порядку роботи (дій або бездіяльності) органів військового управління (командирів та начальників) Збройних Сил України, інших утворених відповідно до законів військових формувань, правоохоронних органів спеціального призначення сектору безпеки і оборони, які виконують згідно чинного законодавства покладені на них службові обов'язки (посадові інструкції).

Об'єктом відповідного виду експертизи є матеріальні носії доказової інформації, які зібрані й надані слідчим або судом на судову військову експертизу.

Основними завданнями військової експертизи є:

– встановлення обставин застосування та дій військових формувань;
– встановлення обставин, що призвели до настання тяжких наслідків, загибелі людей (військовослужбовців, працівників Служби безпеки України, Збройних Сил України, Міністерства внутрішніх справ України, Національної гвардії України та інших представників міністерств і відомств, цивільного населення), втрати озброєння, військової техніки, об'єктів державної влади та інфраструктури, особистого майна громадян під час застосування військових формувань;
– встановлення відповідності дій (бездіяльності) посадових осіб вимогам керівних документів (покладених обов'язків) [5].

Таким чином, вирішуючи вищевказані питання, військова експертиза займає вкрай важливе місце і відіграє спільно з діями правоохоронних органів вирішальну роль у встановленні причин і наслідків правопорушень, вчинених військовими службовими (посадовими) особами, їх взаємозв'язку і, як наслідок, надає можливість законодавчій, виконавчій владі, керівництву сектору безпеки вживати дієвих заходів щодо попередження правопорушень, за які передбачена кримінальна відповідальність.

Список використаних джерел:

1. Актуальні проблеми реалізації політики національної безпеки України в оборонній сфері. Вип. 27 / За заг. ред. В.П. Горбуліна. Київ
ДП НВЦ «Євроатлантикінформ», 2006. 192 с.
2. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 64/2022 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/64/2022 (дата звернення: 19.06.2024).
3. Про оборону України: Закон України від 06.12.1991 № 1932-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1932–12 (дата звернення: 19.06.2024).
4. Конституція (Основний Закон) України: Конституція України; Верховна Рада УРСР від 20.04.1978 № 888-IX // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/888–09 (дата звернення: 19.06.2024).
5. Методика проведення судових військових експертиз щодо оцінки дій посадових осіб (керівників, командирів, начальників)-суб'єктів боротьби з тероризмом, в ході антитерористичної операції: Методика. Київ: КНДІСЕ, 2018 (реєстраційний код 16.1.02).

КРИМІНАЛЬНИЙ ПРОЦЕСУАЛЬНИЙ КОДЕКС-2012 року: КРОК ВПЕРЕД, ДВА НА МІСЦІ

Микола ШУМИЛО
доктор юридичних наук, професор
Заслужений діяч науки і техніки України,
член-кореспондент НАПрН України

Вже більше ніж тринадцять років роботи з Кримінальним процесуальним кодексом (далі – КПК) незалежної України це достатній період часу для тематичних роздумів і висновків. У цьому зв'язку хотів би підтримати думку проф. О.В. Капліної, що контекстно варто згадати й про КПК УСРР 1922 року, ухвалений сто років тому, адже в цьому є певні символіка й логіка. КПК 1922 року дав поштовх становленню кримінального процесу радянського типу, а КПК 2012 року започаткував його руйнацію. На мою думку, співставлення їх вжиткування в різних

соціально-політичних умовах вітчизняної дійсності дозволить більш глибше з'ясувати причини уповільненої адаптації ідей і положень КПК 2012 року у сучасну наукову, нормотворчу та правозастосовну діяльність. Зазначу, що в ХХ столітті в Україні зміна концептуальної рамки розуміння вітчизняного кримінального процесу відбувалася двічі – перший раз із ухваленням КПК УСРР 1922 року, а другий – через 90 років – ухваленням КПК 2012 року. Обидва ці lex ordinandi в своїй долі мають чимало спільного, позаяк ухвалювалися вони в часі конфронтації ідеологічно різних процесуальних парадигм. Але поява нових кодексів ще аж ніяк не означає автоматичної зміни розуміння призначення кримінального процесу як важливого соціокультурного феномену. Не слід забувати й того визначального чинника, що нова «машина» кримінального процесу потребує для свого налаштування певного часу й соціальної підтримки. Дарма що КПК 1922 року опирався на окремі положення дореволюційного законодавства, в цілому він мав вже геть інше ідеологічне забарвлення, зумовлене ідеологемами «побудови соціалізму й комунізму», потребою розбудовувати «радянське право» і створити нову – радянську – парадигму кримінального процесу на основі вже геть інших соціальних цінностей. Головна її особливість полягала в неприхованому диктаті держави над особою, а відтак і свідомому нехтуванні її прав і законних інтересів. Формування цієї парадигми почалося саме з КПК 1922 року, який започаткував був поступове «реформування», а точніше радикальний розрив із доктринальними цінностями СКС 1864 року Тому нема, де правди діти: відбувся справжній ефект «розриву» з попередніми юридичними порядками і правореалізаційними практиками, «дореволюційним минулим», «імперським кримінально-процесуальним законодавством». Відтак був запущений процес цілеспрямованого відходу від засадничих положень судової реформи 1864 року: применшенням ролі суду, ліквідація судового контролю за провадженням досудового слідства; досудове слідство стало доменом органу виконавчої влади; обвинувальна влада стала поволі перебирати на себе функції судової влади; прокуратура організаційно поєднувала в своїй роботі не тільки функції нагляду за дотриманням законності, але й фактичного керівництва досудовим слідством.

Крім змін парадигмального характеру з КПК УСРР 1922 року пов'язано чимало таких негативних практик доктринального характеру, які відтак суттєво вплинули на формування кримінально-процесуального законодавства під радянської України, які, на жаль, нікуди не поділися й до цього часу. Мова йдеться, передовсім, про явище гіперформалізації і надмірної бюрократизації діяльності органів розслідування і судів, що перетворило кримінально-процесуальний закон у «покрокову інструкцію, пам'ятку для малограмотних правозастосувачів». Отже, можна зробити висновок, що КПК УСРР 1922 року по суті свої, був перехідним законом, але саме він який заклав фундамент логічної покрокової – через КПК УСРР 1927 року заміни мішаного кримінального процесу на процес розшукового типу, який знайшов своє остаточне втілення в КПК УРСР 1960 року.

І лише після розпаду Радянського Союзу і здобуттям Україною самостійності в пострадянському кримінальному процесі поступово почали відроджуватися загальновизнані правові цінності. Ідея нового процесуального закону виникла одразу після проголошення Україною незалежності. Внесені зміни до КПК-1960 року в період «малої судової реформи» 2001 року в певній мірі нівелювали його радянську природу, але не змогли істотно вплинути на його ідеологічну платформу. Основа проекту чинного КПК була підготовлена у 2006–2007 роках. Після численних дискусій було визначено, що загальним вектором у розробці нового КПК буде німецька модель кримінального процесу з вкрапленнями окремих англо-американських інститутів (насамперед, hsbeas corpus) [1]. Прикметно, ба більше – знаково, що КПК 2012 року почав далі руйнувати підвалини радянського типу процесу та реанімувати окремі положення СКС 1864 року Це зумовлено тим, що радянські КПК1922, 1927, 1960 р.р. мали стратегічні цілі, геть не сумісні з КПК 2012 року. Перші визнавали «буржуазним хламом» презумпцію невинуватості, змагальність, применшували роль суду шляхом делегування його повноважень органам досудового розслідування і перетворенням його в придаток адміністративно-командної системи. Нехтування загальновизнаними засадничими положеннями кримінального процесу

позначилося на його змістовній характеристиці, що призвело до формування особливої моделі – радянського типу кримінального процесу. До числа його характерних ознак можна віднести: надмірна авторитарність та забюрократизованість процесу, применшення ролі суду, усунення сторони захисту від участі у збиранні та фіксації доказів; невідповідність європейським стандартам процесуального статусу учасників процесу, заформалізованість стадії досудового розслідування, необґрунтоване роз'єднання і як, наслідок дублювання оперативно-розшукової і процесуальної діяльності, пасивна роль прокурора у перебігу досудового провадження, відсутність відповідальності прокурора за проведення розслідування; відсутність судового контролю за діяльністю слідчих органів та міліції; право суду направляти кримінальну справу на додаткове розслідування, відсутність відновного правосуддя; сильний інституційний тиск щодо ухвалення обвинувального вироку. На жаль, на протязі багатьох років деформовані уявлення про кримінальний процес «теоретично обґрунтовувалися» у наукових розвідках, навчальних виданнях, на яких виховалось не одно покоління радянських юристів [2, с. 16].

КПК ж 2012 року взяв курс в стратегічно протилежному напрямку – на «реабілітацію» процесуального і соціального статусу суду, презумпції невинуватості, змагальності, введення на стадії досудового розслідування судового контролю, розподілу процесуальних функцій і інше. КПК 2012 року (як свого часу його історичний попередник – КПК 1922 року) запропонував нову парадигму, спрямовану передовсім на досягнення вже згадуваного мною ефекту «розриву з минулим». Дійсно концептуальний «розрив» відбувся, він має місце, але, на жаль, поки що в тексті закону, але не в правореалізаційній практиці, тобто фактично. Як відомо, проведення кодифікації має на меті в першу чергу усунення правових невизначеностей та забезпечення стабільності в регулюванні відповідних правовідносин. Як свідчить аналіз положень КПК 2012 року і практики його застосування такі функції кодифікації реалізовано не повною мірою. Це може бути пояснено зокрема тим, що певні стереотипи та ідеологеми минулого, закріплені в доктрині і законодавстві, міцно загніздилися в ментальній практиці основної частини юридичної громади, то нема нічого дивного, що вони й далі впливають на процеси розуміння його філософії та тлумачення нового КПК та оновленого іншого процесуального законодавства. Тому КПК – новий, а інструменти для роботи з ним – старі. А це вже проблема зміни методологічних підходів.

Ухвалений у 2012 року КПК можна охарактеризувати як певну спробу реалізувати євро інтеграційні наміри нашої країни в царині кримінальної юстиції у ситуації браку його національної доктринальної моделі, яка б акумулювала в собі як передовий досвід сучасних західних правопорядків, так позитивну вітчизняну практику, ставши відтак надійною теоретичною платформою для здійснення законопроектних робіт. Такий стан речей почасти можна пояснити тим, що після здобуття Україною незалежності вітчизняна теоретична думка силою інерції і перебувала і далі перебуває в сильній залежності від філософії і теоретичних узвичаєнь, на яких був побудований КПК УРСР 1960 року. Тому, як справедливо зазначає один із авторів КПК 2012 року Л.М. Лобойко, кримінально-процесуальна наука геть не була готова думати й діяти в рамках сучасних європейських і англосаксонських традицій в умовах конвергенції правових систем, що є характерним для процесу глобалізації [2, с. 85].

Оскільки життя і наші західні партнери все наполегливіше вимагали підготувати новий КПК, який би міг наблизити вітчизняне правосуддя до критеріїв, розроблених ЄСПЛ, то вирішено було залучити до групи вітчизняних фахівців і зарубіжних колег, які звісна річ, не мали цілісного уявлення про палітру проблем практики українського кримінального судочинства. У цій ситуації, коли, з одного боку, вітчизняна команда проектантів КПК не мала надійної, апробованої юридичною спільнотою теоретичної платформи, а західні консультанти могли лише висловлювати свої рекомендації в рамках власного теоретичного і практичного досвіду, а з іншого, коли підготовлений законопроект не пройшов широкого обговорення в зацікавленому середовищі, й народився «гібридний» КПК, хаотично «склеєний» з фрагментів (запозичень) деяких західних процесуальних інститутів і частин КПК 1960 року, які далеко не завжди – аж до скреготу – належним чином сполучаються між собою. В цьому більше позитиву чим

негативу. Конвергенція різних процесуальних систем в умовах сучасності звичайне явище.

Як бачимо, в КПК 2012 року в порівнянні з КПК 1960 року були запрограмовані радикальні зміни в призначенні, меті і завданнях кримінального процесу; регулюванні правовідносин у царині доказової діяльності, розширенні зони змагальності, істотному корегуванні повноважень окремих учасників кримінального провадження; внесенням раніше невідомих вітчизняному процесу коректив у структуру досудового розслідування, зокрема його початку, запровадженням інституту повідомлення про підозру, належної правової процедури застосування примусових заходів, негласних слідчих (розшукових) дій, компромісних процедур, уточненнями в судових стадіях і інших новацій.

Крім цього, в КПК 2012 року виявилася низка положень, які потребують узгодження та конкретизації задля його логічності та усунення невизначеностей.

Наприклад, загальновизнаним є положення, що ключову функцію у структурі норм кримінального процесуального кодексу відводиться його засадам. Вони визначають ідеологію, архітектоніку, зміст, форму, тип, призначення і мету кримінального провадження. Тому зміст і форма спеціальних норм Кодексу повинні відповідати букві і духу засад кримінального процесу. На жаль, задекларовані у КПК 2012 року окремі засадничі вимоги сучасного європейського зразка, не отримали належної конкретизації у спеціальних нормах, які регулюють процесуальну діяльність у відповідних стадіях провадження, а інколи конфліктують з ними. Це призводить до того, що учасники кримінального провадження нерідко стоять перед складним вибором: приймати вимоги засад кримінального процесу чи далі діяти в дусі надихущих засад законодавства зразка 1960 року Наприклад, ч. 2 ст. 23 КПК закріплено фундаментальне положення: «Не можуть бути визнані доказами відомості, що містяться в показаннях, речах і документах, які не були предметом безпосереднього дослідження суду, крім випадків, передбачених цим Кодексом» [3]. Як на мене, ясніше ясного… Дана норма відповідає вимогам європейської парадигми доказів і доведення, тому відповідно до цього нормативного припису докази можуть формуватися лише в судовому порядку. Визнати чи не визнати матеріали, надані сторонами – це виняткова компетенція судової влади. Крапка. В бо стадії досудового розслідування можуть бути лише матеріали, що можуть претендують на статус судових доказів. Це аксіома європейського доказового права. І вистачить побіжного аналізу норм доказового права у КПК 2012 року, що прийти до невтішного висновку: з одного боку законодавець-реформатор ніби відмовився від моделі доказів радянського кримінального процесу, а з іншого і далі надихався і керувався нею. Подивіться самі. З одного боку, законодавець фактично відмовився від тої вимоги, що кожному різновиду доказів має відповідати встановлений процесуальний режим їхнього збирання. Так, згідно з чинним КПК можна вести мову про наступні варіанти способів отримання доказів: шляхом проведення слідчих (розшукових) дій (ст. ст. 224–245 КПК), негласних слідчих (розшукових) дій (ст.ст. 246–275 КПК), до внесення відомостей в ЄРДР у провадженнях щодо кримінальних проступків (п. 3 ст. 214 КПК). У п. 7 ст. 20 Закону України «Про адвокатуру і адвокатську діяльність» в числі професійних прав адвоката зазначено: «збирати відомості про факти, що можуть бути використані як докази в установленому законом порядку…» [4]. Але з іншого боку, в ч. 1 ст. 84 КПК 2012 року нічтоже сумняшеся відтворено дефініцію поняття доказів, відтворену в Основах кримінального судочинства Союзу РСР та союзних республік у 1958 року, у якій всупереч вимогам п. 2 ст. 23 КПК в числі «продуцентів» доказів вказано прокурора та слідчого. У такий спосіб, як зазначає один із розробників КПК 2012 року В.М. Сущенко «…законодавець вирішив не відмовлятися від традиції КПК-1960 та зберіг термін «збір доказів» на досудовому слідстві, тим самим, хоч і завуальовано, але фактично підтвердивши «обвинувальний ухил» самої стадії досудового слідства, вкотре поставивши під сумнів дієвість конституційного принципу «презумпції невинуватості [5]. Мало того – у нормах, що регулюють діяльність суду першої інстанції, йдеться і про «дослідження доказів, представлених прокурором» (ст. 349 КПК), і «дослідження речових доказів» (ст. 358 КПК), і «з'ясування обставин та перевірка їх доказами (ст. 363 КПК). Вживання в законодавстві таких застарілих словосполучень аж ніяк не узгоджується з вимогами п. 2 ст. 23 КПК.

Висновки: Підсумовуючи, можу сказати, що практика тринадцятирічного функціонування КПК 2012 року підтверджує – мимо всяких зазначених і незазначених його проблемних моментів – слушність задумів його реформаторів, а тому спільним завданням доктрини і законодавця має бути продумане системне корегування його положень у плані реальної, а не лише декларованої орієнтації на кращі європейські стандарти правової організації кримінального судочинства. Для досягнення даної мети, на думку автора, необхідно підготувати збалансовану програму вдосконалення чинного кримінального процесуального кодексу з орієнтацією на німецьку модель кримінального процесу, у якій передбачити: 1) унормування диференціації засад досудового розслідування і судового провадження, зважаючи на їх різну правову природу; 2) узгодженість норм-засад провадження із спеціальними нормами, що регулюють порядок проведення процесуальних дій і прийняття процесуальних рішень у конкретних правовідносинах; 3) приведення у відповідність вимог п. 2 ст. 23 КПК з нормами, що регулюють доказову діяльність у кримінальному провадженні; 4) усунення розбіжностей у правовому регулюванні виявлення і фіксації та вилучення доказових відомостей у провадженнях кримінальних проступків та злочинів; 5) запровадження інституту детективів у органах досудового розслідування; 6) вирішення питання про розумну деформалізації досудового розслідування; 7) уточнення повноважень прокурора в стадії досудового розслідування; 8) врегулювання судового порядку формування доказів.

Список використаних джерел:

1. Банчук О. 5 ідей від розробників КПК, які так і не вдалося втілити у життя. URL: https://justtalk.com.ua/post/5-idej-vid-rozrobnikiv-kpk-yaki-tak-i-ne-vdalosya-vtiliti-u-zhittya? (дата звернення 12.06.2024).

2. Принципи побудови сучасного кримінального процесу України / Н.В. Глинська, Л.М. Лобойко, О.І. Марочкін та ін.: монографія: за заг.ред. О.Г. Шило. Х: НДІ ВПЗ імені акад. В.В. Сташиса НАПрНУ, 2016. 264 с.

3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon5.rada.gov.ua/laws/show/4651–17 (дата звернення: 15.06.2024).

4. Про адвокатуру та адвокатську діяльність: Закон України від 5 липня 2012 року № 5076-VI. URL: https://zakon5.rada.gov.ua/laws/show/4651–17 (дата звернення: 15.06.2024).

5. Сущенко В. Як формувався КПК 2012 року: нотатки автора. URL: https://justtalk.com.ua/post/yak-formuvavsya-kpk-2012-roku-notatki-avtora? (дата звернення: 11.06.2024).

МІЖНАРОДНЕ ПРАВО ТА ВИКОРИСТАННЯ ЗАБОРОНЕНИХ ЗАСОБІВ ВЕДЕННЯ ВІЙНИ

Юлія ЯКОВЕНКО
викладач Національного юридичного
університету імені Ярослава Мудрого

Міжнародне право відіграє ключову роль у регулюванні відносин між державами, забезпечуючи мир та безпеку у світі. Однією з найважливіших його функцій є регулювання використання зброї, особливо тієї, що може завдати надмірних страждань та непоправимої шкоди навколишньому середовищу. Заборонені види озброєння, такі як хімічна, біологічна, ядерна та касетні бомби, ін., підлягають строгому контролю та заборонам згідно з міжнародними договорами та нормами звичаєвого міжнародного гуманітарного права. Розглянемо основні міжнародні правові акти, що регулюють заборону використання цих видів озброєння, а також наслідки їх порушення для міжнародної спільноти.

Міжнародні договори та конвенції.

Одним із найважливіших документів у сфері міжнародного права є Женевські конвенції 1949 року та додаткові протоколи до них, які встановлюють норми гуманітарного права. Вони регулюють захист цивільного населення під час збройних конфліктів та забороняють використання зброї, що спричиняє надмірні страждання або невибіркові руйнування.

1. Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення від 13.01.1993 року.

Конвенція про заборону розробки, виробництва, накопичення і застосування хімічної зброї та про її знищення, підписана у 1993 році, є однією з найважливіших міжнародних угод у сфері контролю над озброєнням. Ця конвенція забороняє використання, виробництво та накопичення хімічної зброї. Держави-учасники зобов'язуються знищити свої запаси хімічної зброї під міжнародним контролем, щоб запобігти її використанню у військових конфліктах або терористичних актах.

Хімічна зброя є однією з найжахливіших форм озброєння через її здатність спричиняти масові страждання, смертельні випадки та довготривалі екологічні наслідки. Такі агенти, як зарин, іприт та VX, можуть спричинити жахливі ушкодження організму, включаючи нервові паралічі, тяжкі опіки шкіри та дихальних шляхів, а також невиліковні хвороби. Використання хімічної зброї під час Першої світової війни та її повторне застосування у різних конфліктах XX століття продемонстрували руйнівну силу цих речовин, що спонукало міжнародне співтовариство до рішучих дій.

Конвенція встановлює чіткі механізми моніторингу та контролю за виконанням зобов'язань, передбачених угодою. Організація із заборони хімічної зброї (ОЗХЗ) здійснює перевірку знищення запасів хімічної зброї та контролює, щоб держави-учасники не порушували умов конвенції. Це включає регулярні інспекції об'єктів, де можуть бути вироблені або зберігатися хімічні речовини, а також проведення розслідувань у випадках підозри на використання хімічної зброї.

Крім того, конвенція сприяє міжнародному співробітництву у сфері хімічної безпеки, обміну інформацією та технологіями для мирного використання хімічних речовин. Держави-учасники зобов'язуються надавати одна одній допомогу у разі загрози або атаки з використанням хімічної зброї, що підвищує рівень колективної безпеки. Серед держав-учасниць є і Україна, яка ратифікувала зазначену конвенцію – 16. 10. 1998 року.

Знищення хімічної зброї є складним та дороговартісним процесом, що вимагає спеціальних технологій і суворого дотримання екологічних норм. Однак більшість держав-учасниць серйозно поставилися до своїх зобов'язань і досягли значних успіхів у знищенні своїх арсеналів хімічної зброї. Це є важливим кроком у напрямку до світу без хімічної загрози.

2. Конвенція про заборону розробки, виробництва і накопичення бактеріологічної (біологічної) і токсичної зброї та про її знищення (КБТЗ) від 10.04.1972 року.

Зазначена конвенція, була прийнята у 1972 році і є одним із найважливіших міжнародних правових документів у сфері контролю над зброєю масового знищення. Ця конвенція забороняє розробку, виробництво та накопичення біологічної зброї та токсинів, які можуть використовуватися як засоби знищення.

Біологічна зброя є надзвичайно небезпечною через її здатність спричиняти масові епідемії та значні людські втрати. Вона включає патогени, такі як бактерії, віруси та інші мікроорганізми, а також токсини, що є продуктами життєдіяльності цих організмів. Наприклад, збудники сибірки, віспи, чуми та ботулізму можуть бути використані як зброя для масового ураження населення, спричиняючи тяжкі хвороби та смерті.

Конвенція була розроблена на основі досвіду минулих війн, коли біологічна зброя використовувалася для завдання значних втрат супротивнику. Однак, потенціал біологічної зброї для неконтрольованого поширення хвороб та її довготривалі наслідки для здоров'я людей і екосистем зробили її використання неприпустимим з точки зору гуманності та міжнародної безпеки.

Одним з ключових аспектів конвенції є її спрямованість на запобігання розробці нових біологічних агентів та токсинів, які можуть бути використані у військових цілях. Це включає зобов'язання держав-учасниць не лише припинити виробництво та накопичення біологічної зброї, але й знищити наявні запаси під міжнародним контролем. Важливим елементом конвенції є також обмін інформацією та технологіями для мирного використання біологічних досліджень, що сприяє міжнародному співробітництву у сфері охорони здоров'я та біобезпеки.

Контроль за виконанням зобов'язань, передбачених конвенцією, здійснюється через систему міжнародних інспекцій та моніторингу. Це дозволяє запобігати можливим порушенням та забезпечувати прозорість у діяльності держав-учасниць. Важливу роль у цьому процесі відіграють міжнародні організації, такі як Всесвітня організація охорони здоров'я (ВООЗ) та Організація Об'єднаних Націй (ООН), які сприяють координації зусиль у боротьбі з біологічними загрозами.

Незважаючи на успіхи у знищенні значних запасів біологічної зброї та зменшенні її поширення, виклики у цій сфері залишаються. Розвиток біотехнологій та генетики створює нові ризики, пов'язані з можливістю створення нових, більш небезпечних біологічних агентів. Тому міжнародне співтовариство повинне продовжувати працювати над удосконаленням механізмів контролю та запобігання використанню біологічної зброї.

3. Договір про заборону Ядерної зброї від 07 липня 2017 року.

На сьогоднішній день діє Договір про заборону Ядерної зброї від 07 липня 2017 року. Проте, на теперішній час його ратифікували лише 70 країн світу, і в цьому переліку немає жодної ядерної держави. Україна також не підписала та не ратифікувала даний договір. Основна мета цього договору полягає у забороні розробки, випробування, зберігання, придбання, транспортування та використання ядерної зброї

Ядерна зброя є найпотужнішою та найруйнівнішою з усіх видів зброї, розроблених людством. Її застосування під час Другої світової війни в японських містах Хіросіма та Нагасакі продемонструвало катастрофічні наслідки для людства та навколишнього середовища, включаючи миттєву загибель сотні тисяч людей, довготривалі наслідки радіаційного зараження та серйозні екологічні пошкодження. Цей досвід підштовхнув міжнародне співтовариство до пошуку шляхів запобігання подальшому поширенню ядерної зброї, зменшення існуючих ядерних арсеналів та її заборони.

Проте, як зазначено в Рекомендаційному висновку Міжнародного суду ООН від 08 липня 1996 року у справі «Законність використання державою ядерної зброї в рамках збройного конфлікту», загроза використання або використання ядерної зброї протирічить загальним принципам МГП, але можливо в екстреній ситуації з метою самооборони.

Зазначений договір є значним кроком у підтриманні спільної безпеки усіх держав світу. Підписання, дотримання та ратифікація договору усіма країнами світу зможе звільнити світ від ядерної зброї та вирівняти становище тих країн, які не є ядерними державами.

4. Конвенція про касетні боєприпаси від 30.05.2008 року.

Конвенція про касетні боєприпаси, прийнята у 2008 році, є важливою міжнародною угодою, спрямованою на заборону використання, виробництва та накопичення касетних боєприпасів. Ці боєприпаси відомі своєю здатністю завдавати невибіркові руйнування та тривалий ризик для цивільного населення через невибухлі суббоєприпаси, які часто залишаються на полі бою після завершення конфлікту.

Касетні боєприпаси складаються з основного контейнера, що містить численні дрібні суббоєприпаси. Після викидання або скидання з літака контейнер розкривається в повітрі, розсіюючи суббоєприпаси на великій площі. Це робить касетні боєприпаси ефективними проти широких військових цілей, але водночас надзвичайно небезпечними для цивільного населення. Часто суббоєприпаси не вибухають одразу після падіння, залишаючись на землі як мінні пастки, що загрожують життю та здоров'ю мирних жителів ще довгі роки після завершення бойових дій.

Конвенція була прийнята на тлі міжнародного обурення наслідками використання касетних боєприпасів у різних конфліктах, таких як війни в Югославії, Іраку та Лівані. Звіт Human

Rights Watch та інших правозахисних організацій показали жахливі наслідки їх застосування, включаючи численні жертви серед цивільного населення та довготривалі руйнування інфраструктури.

Основні положення Конвенції про касетні боєприпаси включають:

1. Заборона використання, виробництва та накопичення. Держави-учасниці зобов'язуються не використовувати, не виробляти, не передавати та не накопичувати касетні боєприпаси. Це є ключовим заходом для запобігання їх подальшому розповсюдженню та використанню у військових конфліктах.

2. Знищення запасів. Кожна держава, що підписала конвенцію, повинна знищити свої запаси касетних боєприпасів протягом визначеного періоду. Це допомагає зменшити ризик їх випадкового або навмисного використання у майбутніх конфліктах.

3. Очищення забруднених територій. Держави-учасниці зобов'язуються здійснювати очищення територій, забруднених невибухлими суббоєприпасами. Це включає виявлення, маркування та знешкодження небезпечних об'єктів, щоб забезпечити безпеку для місцевого населення.

4. Допомога жертвам. Конвенція передбачає надання допомоги жертвам касетних боєприпасів, включаючи медичну допомогу, реабілітацію та соціальну підтримку. Це важливо для забезпечення довгострокової підтримки постраждалих та їхньої інтеграції у суспільство.

Роль міжнародних організацій у виконанні положень Конвенції про касетні боєприпаси є надзвичайно важливою. Організації, такі як ООН, Міжнародний комітет Червоного Хреста та різні неурядові організації, надають технічну допомогу, проводять розмінування територій та надають підтримку постраждалим.

Що стосується війни в Україні, наразі, касетні боєприпаси не заборонені для застосування, як українською армією, так і армією рф, оскільки Конвенція про касетні боєприпаси не ратифікована жодною зі сторін російсько-української війни.

Наслідки порушення заборон.

Порушення міжнародних договорів щодо використання заборонених видів озброєння має серйозні наслідки як для держав-агресорів, так і для міжнародної спільноти в цілому. Держави, що порушують міжнародні договори, можуть стикатися з санкціями з боку міжнародного співтовариства. Це можуть бути економічні, політичні та військові заходи, спрямовані на ізоляцію порушника та примус до дотримання міжнародного права.

Також, особи, відповідальні за використання забороненої зброї, можуть бути притягнуті до відповідальності перед міжнародними судовими органами, такими як Міжнародний кримінальний суд. Це стосується як військових, так і політичних лідерів, які віддавали накази про застосування заборонених видів озброєння.

Крім того, використання заборонених видів озброєння призводить до жахливих гуманітарних катастроф. Загибель мирного населення, руйнування інфраструктури, довготривалі екологічні наслідки – все це результат застосування таких видів зброї.

Висновок

Міжнародне право, спрямоване на заборону використання певних засобів ведення війни, є життєво важливим для забезпечення миру та безпеки у світі. Дотримання цих норм дозволяє зменшити ризики людських втрат та масових руйнувань, сприяє стабільності та розвитку міжнародних відносин. Однак, для ефективного функціонування цих механізмів, необхідно забезпечити суворе дотримання міжнародних договорів усіма державами та невідворотність покарання за їх порушення.

Список використаних джерел:

1. Загурський О.Б. Міжнародна та національна кримінальна відповідальність за використання ядерної зброї//Ядерна безпека: міжнародний та національний вимір: монографія//за заг. ред. ВІ Розвадовського/Авторський колектив: СВ Адамович, ОА Грицан, ОБ Загурський, ВВ

Книш, ВЙ Климончук, ІІ Петровська, ІР Пташник, ВІ Розвадовський; Івано-Франківськ, 2017. § 3.3. С. 242–276.– 2017.

2. Мохончук С.М. Зброя масового знищення як предмет злочину, передбаченого ст. ст. 439, 440 Кримінального кодексу України //Університетські наукові записки.– 2023.– № . 2.– С. 218–223.

3. Пупишева В. Міжнародне гуманітарне право під час російсько-української війни //Актуальні питання права та соціально-економічних відносин Збірник наукових статей.– 2023.– С. 12.

4. Joscelyn, Tom, and Goodman, Ryan. «Let's Talk About Compliance with International Humanitarian Law.» Just Security. May 2, 2024.

5. Whiting, Alex. «Evaluating Proportionality and Long-Term Civilian Harm under the Laws of War.» Just Security. 2024.

6. Нільс Мельцер Міжнародне гуманітарне право. Загальний курс. Делегація МКЧХ в Україні. 2020 р. 396 с. URL: https://blogs.icrc.org/ua/wp-content/uploads/sites/98/2021/05/Nils-Melzer-Comprehensive-introduction-to-IHL-UKR.pdf (дата звернення: 19.06.2024)

7. Договір про заборону Ядерної зброї: Міжнародна конвенція від 07.07.2017 р. URL: https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868/declaration?activeTab=default (дата звернення: 17.06.2024).

8. Законність використання державою ядерної зброї в рамках збройного конфлікту: Консультативний висновок Суду ООН від 08.07.1996 р. URL: https://www.icj-cij.org/sites/default/files/case-related/93/093–19960708-ADV-01–00-EN.pdf (дата звернення: 18.06.2024).

ПРОБЛЕМИ КВАЛІФІКАЦІЇ УЧАСТІ ГРОМАДЯНИНА УКРАЇНИ В ЗБРОЙНИХ ФОРМУВАННЯХ ДЕРЖАВИ-АГРЕСОРА: НАЦІОНАЛЬНЕ І МІЖНАРОДНЕ ПРАВО[1]

Іван ЯКОВЮК
доктор юридичних наук, професор,
професор Національного юридичного
університету імені Ярослава Мудрого
Микола РУБАЩЕНКО
кандидат юридичних наук, доцент,
доцент Національного юридичного
університету імені Ярослава Мудрого

Участь громадянина у військових діях проти власної держави з давніх-давен вважалася тяжким злочином. За КК України 2001 р. ці дії охоплювалися державною зрадою (ст. 111). У березні 2022 р. добровільна участь громадянина України в збройних формуваннях держави-агресора отримала законодавчу оцінку як найтяжчої форми колабораційної діяльності (ч. 7 ст. 111–1). Зі спливом двох років значна частина питань кваліфікації цього виду співпраці з окупантом залишаються дискусійними, мають проблемний характер. У цій доповіді акцентується увага на окремих із них, без претензій на остаточність.

1. Першою проблемою, яка вже була відображена в багатьох наукових працях, є співвідношення вказаної форми колабораційної діяльності із державною зрадою. Основний підхід

[1] Тези підготовлено та опубліковано за грантової підтримки Національного фонду досліджень України в рамках проєкту «Колабораціонізм на тимчасово окупованих територіях України: проблеми правової оцінки, гарантування прав і свобод людини та реінтеграції територій» (проєкт № 2021.01/0106). Проєкт виконується на базі Національного юридичного університету імені Ярослава Мудрого. Зміст, висвітленій у цій публікації може не співпадати з поглядами Національного фонду досліджень України.

до співвідношення колабораційної діяльності і державної зради спирається на те, що загалом перша є спеціальним видом другої. Це судження демонструє лише загальне правило, яке однак, з огляду на різноманіття форм колаборації, передбачених ст. 111–1 КК, і особливості законодавчої конструкції, має декілька винятків, зокрема щодо частин 1 і 6 ст. 111–1.

Стосовно ж аналізованої форми колабораційної діяльності серед науковців і практиків зберігається консенсус щодо визнання добровільної участі у відповідних формуваннях спеціальним (пом'якшуючим) видом державної зради – переходу на бік ворога в умовах воєнного стану (ч. 2 ст. 111 КК). Натомість виникла проблема тлумачення обсягу поняття «добровільна участь». Так, Н.О. Антонюк у контексті добровільної участі громадянина України в складі незаконного збройного формування обмежує цю форму самим лише фактом долучення, входження до складу формувань. На думку дослідниці, якщо ж такий учасник починає здійснювати участь у веденні бойових дій у складі незаконних формувань, то йдеться про вчинення ним або іншої форми колабораціонізму (надання таким формуванням допомоги у веденні бойових дій проти військових формувань України) або ж про вчинення державної зради [2, с. 64]. Такий підхід може мати проєкцію і на добровільну участь в збройному формуванні держави-агресора.

Кваліфікації в означеному випадку воєнного колаборантства (ч. 7 ст. 111–1) за сукупністю з державною зрадою викликає сумніви з позиції природи колабораціонізму: за своєю суттю колабораціонізм є привілейованим видом державної зради, пом'якшення відповідальності за вчинення якого засноване на контекстуальному елементі – умовах окупації території. Це означає, що кваліфікація ведення бойових дій в межах відповідного формування під впливом окупаційного режиму як державної зради не відповідає меті доповнення КК статтею 111–1.

2. Друга проблема побічно пов'язана із першою та обумовлена відсутністю законодавчого визначення колабораційної діяльності та її загальних ознак: чи є обов'язковою ознакою участі громадянина України у збройному формуванні держави-окупанта вчинення цього злочину в умовах окупації (на тимчасово окупованій території)? Відповідь на це питання у наукових джерелах загалом вирішується позитивно. Власне якраз перебування особи в умовах окупації території під час вчинення діяння і є тою обставиною, що дозволяє обґрунтувати появу спеціальної норми і пом'якшення відповідальності за цю форму колабораційної діяльності (ч. 7 ст. 111–1) порівняно із державною зрадою (ч. 2 ст. 111) у зв'язку з екстремальними окупаційними умовами. Це не викликає заперечень за умови, що громадянин України долучився до ворожих збройних сил, перебуваючи в окупації. Однак трапляються випадки, коли він стає їх учасником фактично ще до потрапляння на окуповану територію, наприклад, на «вільній» території України або на території іноземної держави, в подальшому виконуючи покладені на нього завдання на тимчасово окупованій території.

Убачається, що вступ до збройних сил окупанта під час воєнного стану, але поза умовами окупації території, має визнаватися державною зрадою (перехід на бік ворога) і кваліфікуватися за ч. 2 ст. 111 КК. Подальше переміщення особи на тимчасову окуповану територію і перебування в умовах окупації не трансформує більш тяжкий злочин (ч. 2 ст. 111), що вже розпочався, у менш тяжкий (ч. 7 ст. 111–1 КК).

3. Ще одна проблема, яка особливо часто озвучується правозахисниками, полягає в неоднозначному трактуванні законодавчої вказівки на добровільність участі. При тлумаченні посадового колабораціонізму (ч. 5 ст. 111–1) Верховний Суд відмітив, що добровільним слід вважати діяння, яке вчинено при можливості вибрати декілька варіантів поведінки, з урахуванням сукупності обставин, які можуть виключати кримінальну протиправність за приписами статей 39 і 40 КК України [3]. Іншими словами, ця ознака не несе в собі якогось додаткового змісту і радше є додатковим нагадуванням про необхідність врахування загальних норм про фізичний / психічний примус та крайню необхідність під час кримінально-правової кваліфікації.

Трактування цієї ознаки ускладнюється тоді, коли громадянин України, який набув громадянства російської федерації, був призваний для виконання військового обов'язку у складі збройних сил останньої. Призов окупантом громадян окупованої території є порушенням норм міжнародного гуманітарного права та права окупації. Крім того, такі порушення можуть міс-

тити ознаки воєнного злочину, що дає підстави розглядати призваного громадянина як потерпілого (жертву), а не як злочинця.

На наш погляд, слід пам'ятати, що державна зрада та воєнний колабораціонізм належать до найтяжчих злочинів. Автоматичний розгляд громадянина України, призваного на військову службу в збройних силах окупанта, як злочинця чи як потерпілого не може бути виправданим. У кожному конкретному випадку слід з'ясовувати розумність підстав вважати, що особа діяла в умовах крайньої необхідності та чи були перевищені її межі. Те, що призов сам собою має обов'язковий (примусовий в силу вимог законів окупанта) характер, не можна автоматично розглядати як підставу для виключення добровільності в розумінні статей 39 і 40 КК. Разом з тим, факт того, що громадянин вступив до збройних сил окупанта виключно у зв'язку з тим, що відмова потягнула б кримінальну відповідальність за ухилення від призову за законодавством країни окупанта, має бути врахований при індивідуалізації кримінальної відповідальності за ч. 7 ст. 111–1 КК. Питання ж про форму (спосіб) такої індивідуалізації залишається відкритим (йдеться про врахування тяжкості злочину чи таких обставин, що пом'якшують покарання, як вчинення злочину під впливом насильства або в умовах крайньої необхідності при перевищенні її меж?).

4. Ще одне дискусійне питання полягає в тому, який статус з точки зору міжнародного гуманітарного права має громадянин України, який є членом збройних сил російської федерації. Чи має визнаватися він комбатантом та військовополоненим відповідно? Коріння цієї проблеми обумовлено досі триваючими дебатами щодо статусу перебіжчиків в міжнародному гуманітарному праві. Навіть у новому Коментарі до Третьої Женевської конвенції відмічається, що якщо перебіжчики потрапляють під владу держави, з якої вони втекли, то вони все одно отримують статус військовополоненого, але при цьому коментатори підкреслюють відсутність консенсусу і вказують на існування практики, яка вказує на те, що деякі держави виключають статус комбатанта / військовополоненого для перебіжчиків зі своїх власних збройних сил [1].

Наразі можна стверджувати, що в міжнародному гуманітарному праві сформувалися щонайменше дві протилежні позиції з цього питання – одні виступають за визнання їх комбатантами / військовополоненими, а інші – обґрунтовують не поширення цих статусів на перебіжчиків. Вітчизняна ж практика, схоже, демонструє щодо цього прихильність України гуманітарній траєкторії, яка передбачає визнання перебіжчиків комбатантами та військовополоненими відповідно. Як наслідок, виникає проблема правомірності притягнення перебіжчиків до кримінальної відповідальності за участь у збройних силах держави-окупанта з огляду на імунітет комбатанта. Якщо перебіжчики визнаються законними учасниками збройного конфлікту, то вони не підлягають відповідальності за ведення бойових дій, за винятком порушень законів і звичаїв війни. Водночас, перехід на бік ворога (ст. 111 КК) і його спеціальний вид, передбачений ч. 7 ст. 111–1 КК, не є складовою ведення бойових дій, а вказує на порушення обов'язку вірності перед Україною, що дає підстави для обґрунтування правомірності притягнення до кримінальної відповідальності за ці злочини перебіжчиків навіть за умови, що вони визнаються комбатантами.

5. З попередньою проблемою пов'язані також два інших дискусійних питання, які наразі перебувають лише на етапі постановки і потребують більш глибоких досліджень.

Перше стосується можливості видачі іноземній державі (державі-окупанту) військовополонених, які є громадянами України, зокрема в процесі обміну військовополоненими. Конституція України забороняє таку видачу. Проте немає визначеності в тому, чи стосується ця заборона лише процедури видачі в порядку міжнародного співробітництва в кримінальному провадженні, чи вона охоплює також й будь-які інші випадки фактичного передання громадянина під контроль іноземної держави. Так само відсутня ясність і в тому, чи може бажання громадянина на таку видачу виключати застосовність цієї заборони.

Друге стосується більш складного питання про припинення громадянства України і права особи на зміну громадянства. З одного боку, законодавство України про громадянство ґрунтується на принципі визнання права громадянина України на зміну громадянства та передбачає таку під-

ставу втрати громадянства України, як добровільне набуття громадянином України громадянства іншої держави. З іншого боку, припинення громадянства України формально пов'язано виключно з юридичним фактом набрання чинності відповідного указу глави держави щодо конкретної особи. Практика свідчить про превалювання формальної складової над змістовною, водночас це потребує додаткового обґрунтування з точки зору дотримання права на зміну громадянства.

Список використаних джерел:

1. Commentary of 2020 to Geneva Convention (III) relative to the Treatment of Prisoners of War on 12 August 1949, Art. 4 § 996. URL: https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-4/commentary/2020?activeTab=undefined.

2. Антонюк Н.О. Державна зрада і колабораційна діяльність: питання кримінально-правової кваліфікації. Слово Національної школи суддів України. 2021. № 4 (37). С. 64.

3. Постанова Верховного Суду від 31 січня 2024 року, справа № 638/5446/22. URL: https://reyestr.court.gov.ua/Review/116705070. (дата звернення: 18.06.2024)

НЕТОЧНОСТІ ТА НЕВИЗНАЧЕНОСТІ У ТЕКСТІ СТАТТІ 114–2 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

Наталія ЯРМИШ
доктор юридичних наук, професор
співробітник СБУ
Наталія АНГЕЛУЦА
співробітник СБУ

Проблеми, які виникають при вивченні статті 114–2 Кримінального кодексу України (далі – КК України) виявляються вже при ознайомленні з її назвою. Остання розкриває зміст статті з одного боку надто детально, що робіть назву невиправдано громіздкою, з іншого – з відступом від тексту диспозиції. Такий відступ вбачається в тому, що у назві статті йдеться про інформацію щодо розміщення Збройних сил України (далі – ЗС України) чи інших військових формувань, а у диспозиції ч. 2 аналізованої статті для позначення відповідної інформації використовується – «розташування». Відомо, що відповідно до усталених, загально визнаних правил законотворчості текст закону, до якого належать і назви статей, крім іншого, має бути позбавленим синонімів. Тим більше, що з позицій мовознавців, слова, які умовно називають синонімами, тобто такі, що характеризуються однаковим загальним сенсом, насправді мають тонкі відмінності, відрізняються певними відтінками, зокрема ставленням до явищ, що ними визначаються (згадаємо, наприклад так звані синоніми «брехня», «вигадка», «кривда»).

У пояснювальній записці до законопроекту стосовно доповнення КК України статтею 114–2 необхідність цього кроку була аргументована тим, що «ряд громадян України, іноді необдумано (виділено нами: Н.Я., Н.А) та небезпечно здійснюють допомогу ворогу шляхом розповсюдження інформації про направлення, переміщення міжнародної військової допомоги в Україну, а також інформації про переміщення, рух або розташування ЗС України чи інших військових формувань України» [1].

Варто звернути увагу, що відповідні дії автори пояснювальної записки характеризують насамперед, як «необдумані». Далі ті ж самі дії називають «навмисними». Даний законопроект пропонувалось прийняти «з метою встановлення справедливого покарання для осіб, які здійснюють навмисне та незаконне розповсюдження інформації про направлення, переміщення міжнародної військової допомоги в Україну, а також інформації про переміщення, рух або розташування ЗС України чи інших військових формувань України» [1].

Вочевидь, мається на увазі, що людина, яка поширює зазначену інформацію розуміє фактичний характер своїх дій (це випливає з оцінки їх як умисних), проте не замислюється над тим, до чого вони можуть призвести. Адже автори законопроекту визначають їх як «необдумані». Проте за таких умов навряд чи коректним буде називати поведінку «пособництвом державі-агресору» [1], адже пособництво є цілеспрямованою дією.

Розгляд пояснень, що містяться в аналізованій записці, веде до думки, що описані в законопроекті (а зараз вже в чинному законі) дії, об'єктивно здатні допомогти ворогу в його агресії проти України, проте в суб'єктивному аспекті такою метою не характеризуються.

Як очевидний дисонанс з уявленнями авторів розглядуваного законопроекту про «необдуманість» поширення відповідної інформації сприймається ознака ч. 3 ст. 114–2 КК України: «Дії, …, вчинені… з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням…». Виникає риторичне запитання: про яку «необдуманість» поширення певної інформації, йде мова, якщо це здійснюється «з метою надання такої інформації». Та чи доречно при цьому говорити про «поширення»? Риторичний характер цього запитання визначається тим, що «мета» передати інформацію ворогу та «необдуманість» – поняття несумісні. Одразу ж звернемо увагу і на несумісність слів «поширення» та «комусь» (в статті «поширення державі-агресору чи її представникам»). А саме до таких внутрішньо суперечливих виразів веде конструкція ч. 3 ст. 114–2 в аспекті «поширення з метою передачі…».

Частини перша та друга ст. 114–2 є самостійними складами злочинів, оскільки передбачають поширення інформації різного змісту. У ч. 1 цієї статті вказана інформація про «направлення, переміщення зброї, озброєння та бойових припасів в Україну, в тому числі про їх переміщення територією України». Отже, предметом даного складу злочину така інформація є лише у разі, якщо вона «не розміщувалася (не поширювалася) у відкритому доступі…».

Тлумачення виразу «не розміщувалася (не поширювалася) у відкритому доступі», має принципове значення, оскільки надає можливість зрозуміти поняття «поширення» в будь-якому контексті. Слід замислитись, чи дійсно законодавець адекватно розтлумачив слово «поширення». До слів «не розміщувалася» законодавець в дужках додає «не поширювалася». Тим самим він фактично застосовує слова «розміщення» та «поширення» як синоніми. Проте чи є вони такими насправді? Чи будь-яке розміщення є поширенням? Чи не може певна інформація бути розміщена у закритих документах, в обмеженому доступі? Звісно ж – може. Але поширенням це назвати важко. Вочевидь, законодавець намагався сказати, що поширенням є розміщення інформації виключно у відкритих джерелах. В такому разі, він неправильно обрав місце для слова, що наводить у дужках. Логічно, правильно було б казати: «якщо ця інформація не розміщувалася у відкритому доступі (не поширювалася). Стає цілком зрозуміло, що поширенням інформації є не будь-яке її розміщення, а розміщення саме у відкритому доступі.

Якщо законодавець розкриває поняття «поширення», то інакше як «розміщення у відкритому доступі» його не можна. Якщо так, то і поширення відповідної інформації суб'єктом розглядуваного злочину, як ознаку об'єктивної сторони його складу, також слід розуміти як розміщення її саме у відкритому доступі. А це ще один аргумент на користь того, що передбачене у ч. 3 поширення інформації з метою її надання державі-агресору – це нонсенс. Інформацію можна або поширити (розмістити у відкритому доступі), або передати комусь. Звісно, суб'єкт, розмістивши інформацію у відкритому доступі, втрачає над нею свій контроль, тому вона може стати надбанням кого завгодно, зокрема і представника ворожої країни. Але з метою надання це несумісне. У Єдиному державному реєстрі судових рішень зустрічаються вироки, де особа, яка за завданням представника ворожої країни збирала та передавала йому відповідну інформацію, була засуджена за ч. 3 ст. 114–2 з поясненням, що вона вчинила дії, «по'вязані з поширенням інформації представнику держави, що здійснює збройну агресію проти України…» [2]. Враховуючи викладене вище, таку кваліфікацію слід визнати помилковою. Можна погодитися з тими судами, які в аналогічних ситуаціях кваліфікують дії суб'єкта як державну зраду. Так, дії суб'єкта, які полягали в тому, що на виконання злочинного завдання представника розвідки

ворога він отримував (фотографував) та передавав дані про місця дислокації та переміщення підрозділів ЗС України, були визнані наданням допомоги представнику іноземної держави у проведенні підривної діяльності проти України, вчиненої в умовах воєнного стану та кваліфіковані за ч. 2 ст. 111 КК України.

Вважаємо, що такі, неприпустимі, розбіжності у кваліфікації однакових за ключовими моментами дій, походять від законодавчої помилки у формулюванні відповідної ознаки ч. 3 ст. 114–2 КК України. Тому кваліфікуючу ознаку «дії, передбачені частиною першою або другою цієї статті, вчинені…з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням» з ч. 3 ст. 114–2 доцільно прибрати.

Підлягають обговоренню і співвідношення ознак предмету складів розглядуваних злочинів. У ч. 1 ст. 114–2 йдеться про інформацію щодо «направлення, переміщення…зброї, озброєння та бойових припасів», у ч. 2 – щодо «переміщення, рух або розташування Збройних сил України чи інших…військових формувань».

Зауважимо, що у ч. 1 йдеться лише про певну динаміку: направлення, переміщення, тобто рух (хоча останнього слова у ч. 1 немає), а у ч. 2 – і про «статику» (крім переміщення та руху збройних сил зазначено й їхнє «розташування»). Таким чином, якщо справа стосується зброї, озброєння чи бойових припасів, то інформація про їх розташування не підпадає під ознаки складу злочину, передбаченого ч. 1 ст. 114–2. Зрозуміло, що поширення інформації про розташування зброї озброєння, боєприпасів не підпадає і під ознаки ч. 2 цієї статті, оскільки остання передбачає інформацію, що стосується ЗС України чи інших військових формувань. Таким чином, поширення інформації щодо розташування зброї, озброєння або бойових припасів цілком виключає можливість застосування до особи ст. 114–2. Залишається можливість розглядати поширення відповідної інформації в якості державної зради, проте справедливість такої кваліфікації викликає сумніви через відсутність цілеспрямованості такої поведінки. Адже поширена інформації про розташування зброї не обов'язково може опинитися «у руках» ворога, тут може спрацювати випадковість.

Обговоримо, які складнощі виникають стосовно саме предметів (речей) направлення чи переміщення яких стосується інформація, поширення якої передбачено у ч. 1 ст. 114–2. Це зброя, озброєння та боєприпаси. Даний перелік вичерпний. А це вимагає правозастосовника чітко вказувати, інформація про направлення чи переміщення яких саме предметів поширена суб'єктом. Тим більше, що у ч. 2 ст. 114–2 зазначена інформація вже не про речі, а про певні формування, а саме ЗС України та інші військові формування. Виникає питання, до якої категорії належить військова техніка? Це озброєння чи ЗС (або інші військові формування)? Від розв'язання цього питання залежить, зокрема, наявність чи відсутність складу злочину, передбаченого ст. 114–2 у разі, якщо була поширена інформація не про направлення чи переміщення цієї техніки, а про її розташування. Повторимо, що в частині 1 аналізованої статті розташування не зазначено. Тому якщо навіть визнати військову техніку чи зброєю, чи озброєнням, чи бойовими припасами, то поширення відповідної інформації про її розташування під ознаки ч. 1 ст. 114–2 не підпадає. Вивчення тексту ЗУ «Про Збройні Сили України» схиляє до висновку, що військова техніка до озброєння не належить. Так, серед повноважень Кабінету Міністрів України стосовно ЗС України (абз. другий ст. 9) зазначено, що він «забезпечує постачання ЗС України озброєння, військової техніки…» [3]. Як бачимо, військова техніка тут перебуває за межами озброєння.

Залишається спроба розглянути військову техніку в аспекті ч. 2, тобто визнати її як «ЗС України чи інші військові формування». Вирок, щодо особи, яка фотографувала та розміщувала у відкритому доступі приховану, зокрема на території дитячого табору, військову техніку. У вироку ця інформація позначена як «інформація військового характеру», з уточненням, що це «інформація про місце розташування військової техніки ЗС України». А у підсумку зафіксовано, що особа, яка поширила цю інформацію, «обґрунтовано обвинувачується у поширенні інформації про розташування ЗС України…» [4]. Тобто військова техніка була визнана саме як ЗС України. Аргументація такого тлумачення у вироку відсутня.

Водночас віднесення військової техніки до ЗС України (принаймні коли йдеться виключно про техніку) є принципово важливим. З ч. 1 ст. 1 ЗУ «Про Збройні Сили України» однозначно вбачається, що ЗС України – це насамперед люди. Саме вони, навіть і без військової техніки (якщо так склалося) зобов'язані захищати нашу Україну. Якщо ж техніку без людей не можна вважати ЗС України (чи іншими військовими формуваннями), а також не розглядати як озброєння, то застосування ст. 114–2 до осіб, які поширили інформацію про розташування цієї технікі взагалі застосовувати не можна.

Як бачимо, визнання належності певних предметів до тих, що передбачені у ч. 1 чи 2 ст. 114–2 має принципове, а для особи, що поширює відповідну інформацію,– доленосне значення. Адже санкція ч. 2 більш сувора. Тому, визнання, зокрема, техніки військовим формуванням означає більш сувору відповідальність, а невизнання, тобто віднесення до зброї, озброєння чи боєприпасів – за відсутності «руху», «переміщення» взагалі не тягне відповідальності за ст. 114–2. До того ж, виявляється й те, що під сумнівом й віднесення військової техніки до озброєння. Звісно ж, відповідні ознаки підлягають ретельної корекції.

Виходячи з міркувань необхідності певного узагальнення предметів, передбачених у ч. 1 ст. 114–2, проектанти нового КК України запропонували у відповідній статті (9.2.3) іменувати їх «товарами військового призначення». Проте, здається, така назва є не зовсім вдалою. Слово «товар» зміщує акцент на властивості речей бути предметом обміну. А в даному контексті це має бути їх призначення як засіб захисту від агресора. Тому вважаємо за доцільне сформулювати відповідну ознаку, наприклад так, як це зроблено у назві пояснюваної записки «До проекту ЗУ «Про внесення змін до статті 114–2 КК України щодо удосконалення відповідальності за несанкціоноване розповсюдженню інформації про засоби протидії збройній агресії Російської Федерації». Можна і декілька скоротити, трансформувати визначення, назвати відповідні речі засобами ведення бойових дій чи засобами військового призначення. Це значно полегшило б застосування ч. 1 ст. 114–2 КК України.

Щодо ознак ч. 2 цієї статті варто обговорити й те, що у її диспозиції зазначено, що інформація, яка поширюється суб'єктом, має бути такою, аби її можна було б ідентифікувати на місцевості. У ч. 1 така вимога відсутня. Під час доопрацювання ст. 114–2 КК України, що є вкрай необхідним і сприятиме більш ефективному захисту інформаційної безпеки, законодавцю варто замислитися й стосовно цього аспекту.

Список використаних джерел:

1. Пояснювальна записка до проекту Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому розповсюдженню інформації про направлення, переміщення міжнародної військової допомоги в Україну, рух, переміщення або розміщення Збройних Сил України чи інших військових формувань України, вчинене в умовах воєнного або надзвичайного стану» URL: blob: https: //itd.rada.gov.ua/2e354273–6c3d-4ac3-a44d-c1be9e9cf1f1 (дата звернення: 20.06.2024).

2. Вирок Обухівського суду Київської області від 10 листопада 2023 р. Справа № 372/2509/23. Провадження 31-кп-273/23 URL: https: //reyestr.court.gov.ua/Review/114823130 (дата звернення: 20.06.2024).

3. Про Збройні Сили України: Закон України від 06.12.1991 № 1934-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1934–12 (дата звернення: 20.06.2024)

4. Вирок Слов'янського міськрайонного суду Донецької області від 29 грудня 2022 року. Провадження № 1-кп/243/587/2022 URL: https://reyestr.court.gov. ua/Review/108172224 (дата звернення: 20.06.2024).

Секція 2
СУЧАСНА ПАРАДИГМА КОНТРРОЗВІДУВАЛЬНОЇ ТА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ: ДО ПИТАННЯ СУЧАСНОГО ДОКТРИНАЛЬНОГО ВИЗНАЧЕННЯ

Сергій АЛБУЛ
кандидат юридичних наук, професор,
професор кафедри оперативно-розшукової
діяльності факультету підготовки фахівців
для підрозділів кримінальної поліції
Одеського державного університету
внутрішніх справ

З набуттям Україною незалежності почалося формування вітчизняної правової бази у всіх галузях суспільного життя. Розвиваючись в нових соціальних умовах, правова система нашої держави стикнулася з необхідністю кардинальної зміни парадигми, швидкого подолання законодавчих протиріч та застарілого радянського світогляду. Правова регламентація оперативно-розшукової діяльності, її фактична легітимізація, розроблення, обґрунтування та формування основних правових концептів розвивалися одночасно з процесами державотворення сучасної України. Орієнтуючись на досвід провідних країн світу, теоретичні положення суміжних галузей знань, напрацювання науковців, вперше в історії України 18 лютого 1992 року був прийнятий Закон «Про оперативно-розшукову діяльність», який на довгі роки став базовим щодо її регламентації.

Легітимізація оперативно-розшукової діяльності шляхом прийняття відповідного Закону закріпила її правовий статус та вивела на новий рівень, позбавивши таємні відомчі нормативні акти функції основного регулятора. Разом із тим, Закон України «Про оперативно-розшукову діяльність», відповідаючи вимогам юридичної техніки, не є сталим правовим актом і за час свого існування неодноразово піддавався змінам та доповненням. Нагальна потреба розроблення та прийняття нового, сучасного Закону України «Про оперативно-розшукову діяльність» назріла вже давно [1, с. 159]. При цьому, дослідники відмічають активну законопроєктну увагу з боку Верховної Ради України до питань оновлення оперативно-розшукового законодавства [3, с. 141–144].

З моменту набрання чинності до вказаного Закону сорок вісім разів вносилися відповідні зміни та доповнення. Крім цього, комітетами Верховної Ради України були опрацьовані та розглянуті наступні законопроєкти:

– від 17 лютого 2015 р. № 2153 «Про внесення змін до статті 9–2 Закону України «Про оперативно-розшукову діяльність» (щодо підстав закриття оперативно-розшукових справ)»;
– від 06 квітня 2015 року № 2555 «Про внесення змін до законів України, що регулюють оперативно-розшукову та контррозвідувальну діяльність»;
– від 12 травня 2015 року № 2804 «Про внесення змін до деяких законодавчих актів України щодо надання органам Військової служби правопорядку у Збройних Силах України

повноважень на здійснення досудового розслідування кримінальних правопорушень та здійснення оперативно-розшукової діяльності»;
- від 04 червня 2015 року № 2024а «Про внесення змін до деяких законодавчих актів України щодо оперативно-розшукової діяльності в органах і установах виконання покарань, слідчих ізоляторах»;
- від 06 липня 2015 року № 2292а «Про внесення змін до Закону України «Про оперативно-розшукову діяльність» щодо підрозділів, які провадять оперативно-розшукову діяльність»;
- від 03 червня 2016 року № 4778 «Про оперативно-розшукову діяльність»;
- від 04 квітня 2017 року № 6284 «Про оперативно-розшукову діяльність»;
- від 02 вересня 2019 року № 1229 «Про оперативно-розшукову діяльність» [6].

Слід наголосити, що доля вказаних законопроєктів невтішна – після доопрацювань та обговорень більшість з них було відхилено та знято з розгляду.

Теоретичні джерела закріплюють, що правова дефініція – це нормативно-правовий припис, який детально визначає сутнісний зміст правового поняття шляхом опису його основних юридично значущих ознак або елементів з метою забезпечення єдності правового розуміння та регулювання [12]. На сьогодні теорія ОРД оперує поняттям «оперативно-розшукова діяльність», яке закріплено на законодавчому рівні. З моменту прийняття та набрання чинності Законом України «Про оперативно-розшукову діяльність», майже двадцять вісім років поспіль оперативно-розшукова діяльність визначалася як система гласних і негласних пошукових, розвідувальних (курсив наш – С.А.) та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів.

У 2020 році Верховною Радою України було прийнято Закон України «Про розвідку» [7]. З його прийняттям та набранням чинності з поняття оперативно-розшукової діяльності було виключено розвідувальну складову. Таким чином, на сьогодні стаття 2 Закону України «Про оперативно-розшукову діяльність» закріплює, що оперативно-розшукова діяльність – це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів [5]. Разом із тим, само поняття «оперативно-розшукової діяльності» не зазнавало сутнісного, доктринального переосмислення як правова дефініція.

За нашим переконанням, питання щодо теоретичних концептів формування правової дефініції оперативно-розшукової діяльності необхідно аналізувати крізь призму вимог та положень юридичної техніки, а саме таких, що стосуються логіки та мовних правил правового акту. Як вказують фахівці, «забезпечення логіки пов'язано з тією обставиною, що правовий акт містить у собі модель того процесу, який покликаний регулювати правовідносини та логіку поведінки його учасників. Від рівня логіки правового акту залежить і рівень регулювання моделі поведінки».

У свою чергу, мовні правила пов'язані з тим, що мова становить собою основний засіб передачі будь-якої інформації та є зовнішньою формою будь-якого змісту. Мова права має певні особливості, до яких належить: офіційність, ясність, точність, однозначність, повнота змісту, нормативність та стабільність, а також забезпечення відсутності двозначності у трактуванні правових норм. Отже, правова дефініція має містити чіткі формулювання, окреслювати логічно обґрунтовані сутнісні ознаки правової категорії. З огляду на це, за нашим переконанням, на сьогодні правова дефініція «оперативно-розшукова діяльність», що міститься у ст. 2 Закону, не розкриває таких сутнісних ознак та не в повній мірі відповідає вимогам юридичної техніки.

Існуюча правова дефініція закріплює, що оперативно-розшукова діяльність – це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів [5]. Спробуємо детально проаналізувати зазначену дефініцію. Автори «Філософського енциклопедичного словника» вказують, що система – це множина взаємопов'язаних елементів, що утворюють єдине ціле, взаємодіють із середовищем та між собою, і мають мету [11, с. 621]. У нашому випадку такими елементами

системи виступають гласні та негласні пошукові та контррозвідувальні заходи. Тобто, по суті, складовими поняття є система інструментів (заходів), за допомогою яких вирішуються певні завдання. Такими завданнями, відповідно до ст. 1 Закону, є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [4, с. 23]. Доводиться констатувати, що у існуючій дефініції вітчизняний законодавець фактично лише перелічує наявний інструментарій для реалізації завдань оперативно-розшукової діяльності, не розкриваючи сутнісні ознаки правової категорії, а також праксеологічну сутність ОРД, що, на нашу думку, є концептуальним недоліком.

Філософія практичної діяльності розглядає праксеологію, як науку, галузь досліджень, що вивчає людську діяльність, процеси прийняття рішень крізь призму їх ефективності [11, с. 512]. У свою чергу, діяльність – це процес активної взаємодії суб'єкта з об'єктом, під час якого суб'єкт досягає певної мети [11, с. 163]. З огляду на це, ми впевнені, що сучасне доктринальне визначення оперативно-розшукової діяльності має розкривати її сутнісні ознаки саме у площині праксеології.

Досліджуючи праксеологічні аспекти означеної правової дефініції, необхідно, на наш погляд, проаналізувати і поняття «діяльності», адже сучасні наукові джерела містять різнопланові визначення, що розкривають її сутнісні ознаки. Діяльність це є активна, свідома, вольова поведінка, система доцільних, спланованих дій, спрямованих на реалізацію визначених задач та досягнення певної мети. Інакше кажучи, діяльність є особливою формою активності людини. Аналізуючи сутність категорії «державна діяльність», науковці зазначають, що такою є діяльність державних організацій (органів, установ, підприємств, їх представників та службовців), спрямована на реалізацію функцій держави, структура змісту якої (суб'єкти, способи, мета, засоби, результат тощо) виявляється у правових та неправових формах відповідно до сутності та соціального призначення держави [10, с. 225]. У свою чергу, автори підручника «Судова, правоохоронна та правозахисна системи України» вказують, що правоохоронна діяльність – це вид державної діяльності, яка здійснюється з метою охорони права спеціально уповноваженими органами шляхом застосування юридичних заходів впливу в суворій відповідності з законом і при неухильному дотриманні встановленого ним порядку [9, с. 17]. Інші науковці зазначають, що правоохоронна діяльність – це діяльність спеціально уповноважених органів (державних та недержавних) з метою охорони прав і свобод громадян, правопорядку та забезпечення законності, що реалізується в установленій законом формі та в межах повноважень, наданих цим органам [10, с. 224].

Чинний Закон України «Про контррозвідувальну діяльність» закріплює, що такою є спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України [2, с. 3].

У свою чергу, розвідувальна діяльність розглядається як діяльність, що здійснюється спеціальними засобами і методами з метою забезпечення визначених законом органів державної влади розвідувальною інформацією, сприяння реалізації та захисту національних інтересів, протидії за межами України, у тому числі у кіберпросторі, зовнішнім загрозам національній безпеці України [8]. Як бачимо, у всіх цих визначеннях чітко простежується праксеологічна складова, що вбачається нам виправданим і таким, що має бути обов'язково враховано у правовій дефініції «оперативно-розшукова діяльність». Таким чином, до сутнісних ознак правової дефініції «оперативно-розшукова діяльність», за нашим переконанням, належать: державний, владний характер; суб'єктний склад; мета такої діяльності.

Враховуючи вищевикладене, на наш погляд, оперативно-розшукову діяльність можна визначити як діяльність спеціально уповноважених державних органів щодо організації та проведення гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів, з метою пошуку і фіксації фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій, припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави.

Список використаних джерел:

1. Албул С.В. Оперативно-розшукова діяльність: до питання новелізації правової дефініції. Роль та місце правоохоронних органів у розбудові демократичної правової держави: матеріали XVI Міжнародної науково-практичної інтернет-конференції. (м. Одеса, 29 березня 2024 р.) Одеса: ОДУВС, 2024. С. 159–162.

2. Албул С.В. Правові засади контррозвідувальної діяльності в Україні. Південноукраїнський правничий часопис. 2023. № 2. С. 3–7. DOI https://doi.org/10.32850/sulj.2023.2.1

3. Гнєтнєв М., Білецький В., Басалик С. Законопроектна увага до оперативно-розшукової діяльності з боку Верховної Ради України VIII скликання. Вісник Національної академії Державної прикордонної служби України. 2018. № 4. С. 141–144.

4. Оперативно-розшукова діяльність: навчальний посібник / С.В. Албул, С.О. Єгоров, Є.В. Поляков, Т.Г. Щурат; за заг. ред. проф. С.В. Албула.– Одеса: ОДУВС, 2023.– 375 с. (Серія: Теорія і практика ОРД).

5. Про оперативно-розшукову діяльність: закон України від 18.02.1992 № 2135-XII із змін. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2135–12/print (дата звернення 02.06.2024).

6. Про оперативно-розшукову діяльність: проєкт закону України від 02.09.2019 № 1229 [Електронний ресурс]. URL: http: //w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66597 (дата звернення 02.06.2024).

7. Про розвідку: закон України від 17.09.2020 № 912-IX [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/912–20/print (дата звернення 02.06.2024).

8. Розвідувальна діяльність. Вікіпедія [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Розвідувальна_діяльність (дата звернення 02.06.2024).

9. Судова, правоохоронна та правозахисна системи України: підручник / С.В. Албул, М.О. Баймуратов, А.І. Берлач та ін.; за заг. ред.д.ю.н., проф. С.О. Кузніченка. Одеса: ОДУВС, 2012. 402 с.

10. Тихонова Д.С. Поняття «правоохоронна діяльність» і функції правоохоронної діяльності. Проблеми сучасної поліцеїстики: матеріали науково-практичної конференції (Харків, 20.04.2022). Харків: ХНУВС, 2022. С. 224–225.

11. Філософський енциклопедичний словник / НАН України, Ін-т філософії ім. Г.С. Сковороди; за ред. В.І. Шинкарук. Київ: Абрис, 2002. 742 с.

12. Хворостянкіна А.В. Дефініції в законодавчих текстах: питання теорії. Офіційний сайт Міністерства юстиції України [Електронний ресурс]. URL: https://minjust.gov.ua/m/str_6669 (дата звернення 02.06.2024).

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ДОПОМОГИ ГРОМАДЯН У ПРОТИДІЇ СЛУЖБОВИМ ПРАВОПОРУШЕННЯМ СПІВРОБІТНИКІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Артем БУДНІК
співробітник СБУ

Для належного виконання завдань з протидії службовим правопорушенням у підрозділах Служби безпеки України (далі – СБУ) важливу роль відіграє налагодження конфіденційної співпраці з громадянами, які можуть надавати оперативну інформацію співробітникам підрозділів внутрішньої безпеки СБУ (далі – ПВБ СБУ). Така робота є складовою оперативно-розшукової діяльності (далі – ОРД) та передбачена законодавством України.

Особи, які на довірчих засадах конфіденційно співпрацюють з ПВБ СБУ, можуть надавати первинні відомості про події та факти правопорушень співробітників СБУ, сприяти у проведенні оперативно-розшукових заходів, легалізувати оперативну інформацію тощо. Їх допомога може мати тимчасовий або тривалий характер залежно від взаємної домовленості.

Ефективність використання таких осіб ПВБ СБУ значною мірою залежить від дотримання принципу конспірації. Об'єкти оперативного інтересу часто мають високий рівень професійної підготовки та здатні протидіяти спецслужбі. Тому організація та проведення роботи з довіреними особами потребує ретельної підготовки, вибору безпечних місць, розробки легенд тощо.

Серед основних труднощів у цій роботі – складність встановлення та підтримання довірчих відносин у середовищі співробітників СБУ, брак сучасної методичної бази, підбір надійних довірених осіб, забезпечення конспірації зустрічей. Важливим є також питання забезпечення безпеки довірених осіб від протиправного тиску з боку об'єктів оперативного інтересу.

Чинне законодавство України потребує вдосконалення в частині врегулювання порядку налагодження конфіденційної співпраці з громадянами, які сприяють ПВБ СБУ, та забезпечення їх безпеки на етапі ще до відкриття кримінального провадження. Необхідно створити дієві механізми державного захисту таких осіб на рівні закону.

Отже, робота з довіреними особами є важливою складовою діяльності ПВБ СБУ. Проте чинне законодавство України не повною мірою врегульовує питання забезпечення безпеки громадян, які конфіденційно співпрацюють з органами СБУ.

Чинний Закон України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» передбачає державний захист для таких осіб лише у рамках кримінального процесу [1]. Однак, на практиці конфіденційне співробітництво розпочинається ще до порушення кримінального провадження, під час збору первинної інформації. Тому слово «конфіденційний» не охоплюється всіма аспектами конспірації, необхідними для безпеки таких громадян.

Крім того, у згаданому Законі не розкривається зміст терміну «конфіденційність», а лише зазначено, що таким особам гарантується державний захист у разі розголосу їх персональних даних (п. «ж» ч. 1 ст. 7). Втім, розголошення інформації про особисту безпеку та життя цих громадян є більш серйозним порушенням режиму конфіденційності.

На думку правників, положення чинного Закону потребують ретельного вивчення та доопрацювання з метою забезпечення ефективного захисту осіб, які беруть участь у кримінальному процесі та надають допомогу правоохоронним органам на всіх етапах досудового розслідування злочинів.

Так, у п. «д1» ч. 1 ст. 2 Закону [1] після слів «викривач» доцільно додати фразу «а також особи, які на конфіденційних засадах надають допомогу органам досудового розслідування». Це дозволить розширити коло осіб, які підпадають під дію Закону.

Важливим аспектом використання допомоги осіб, які сприяють ПВБ СБУ є належний відбір та підготовка таких осіб. Під час добору кандидатів на довірче співробітництво оперативні працівники мають звертати увагу на їхні особистісні якості, обізнаність у специфіці правопорушень співробітників СБУ, можливості для отримання оперативної інформації та ін.

Зокрема, потенційними довіреними особами можуть стати особи, які через свій службовий статус не мають можливості отримувати незаконні доходи, але водночас володіють інформацією про протиправні дії інших співробітників СБУ. Особливу увагу при доборі варто приділяти особам, котрі самі не вчиняли правопорушень та мають позитивне ставлення до Служби безпеки.

Успішна реалізація конфіденційної співпраці з громадянами потребує від ПВБ СБУ постійної роботи з удосконалення методик цієї роботи, підвищення професійного рівня особового складу, створення сучасної методичної бази з врахуванням новітніх технологій та інформаційної безпеки.

Ще одним важливим аспектом використання допомоги громадян ПВБ СБУ є питання належної оплати та мотивації їх співпраці. На жаль, наразі державна винагорода для таких осіб не відповідає сучасним ринковим реаліям.

Слід враховувати, що особи зазначеної категорії можуть мати доступ до інформації про високопосадовців та співробітників СБУ, причетних до корупційних схем та отримання значних незаконних доходів. У такому випадку запропонована оперативниками мізерна винагорода за співпрацю навряд чи виглядатиме привабливою.

Тому одним із шляхів підвищення ефективності роботи з особами, які сприяють діяльності ПВБ СБУ може стати перегляд системи їх грошової винагороди та приведення її у відповідність до реального рівня матеріальної забезпеченості потенційних джерел інформації. Розміри оплати співпраці мають бути економічно обґрунтованими та конкурентоспроможними на противагу можливим пропозиціям з боку злочинного середовища.

Разом з тим, мотивація до співпраці з ПВБ СБУ не повинна обмежуватись лише фінансовою винагородою. Важливим стимулом є також забезпечення їхньої особистої безпеки від протиправного тиску та розголошення даних про конфіденційну співпрацю.

Тому паралельно зі вдосконаленням законодавчих механізмів державного захисту таких осіб, оперативним співробітникам ПВБ СБУ доцільно докладати максимум зусиль для збереження в таємниці інформації про факт і деталі конфіденційної співпраці. Будь-яке порушення конспірації створює прямі загрози життю та здоров'ю довіреної особи і членів її родини.

Підсумовуючи, слід зазначити, що налагодження ефективної роботи з особами, які на добровільних засадах сприяють діяльності ПВБ СБУ, потребує комплексного підходу з боку зазначених підрозділів. Це стосується як удосконалення законодавчого поля, так і розробки дієвих оперативно-тактичних прийомів та підвищення професійного рівня особового складу.

Підбиваючи підсумки, можна зазначити, що налагодження ефективної роботи з довіреними особами є одним з ключових факторів успішної протидії службовим правопорушенням співробітників СБУ. Проте наразі в цій сфері існує низка проблемних питань, які потребують комплексного вирішення.

По-перше, важливим є удосконалення законодавчої бази щодо забезпечення безпеки громадян, які на конфіденційних засадах співпрацюють з правоохоронними органами. Доцільно внести зміни до Закону «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», розширивши його дію також на осіб, які сприяють органам досудового розслідування до порушення кримінальної справи.

По-друге, ПВБ СБУ необхідно активізувати роботу з підбору та підготовки довірених осіб. Ретельний відбір потенційних джерел інформації за особистісними та професійними критеріями, якісний інструктаж з питань конспірації та взаємодії є запорукою отримання достовірних оперативних відомостей.

По-третє, вкрай важливим залишається питання належного матеріального стимулювання осіб, які добровільно сприятимуть діяльності ПВБ СБУ. Розміри винагороди мають бути еко-

номічно обґрунтованими та конкурентоспроможними порівняно з можливою протиправною вигодою.

Також слід приділити увагу підвищенню рівня професійної майстерності оперативних працівників ПВБ СБУ у сфері конспіративної роботи з такими особами, опанування новітніх методик та технологій безпечної комунікації.

Лише комплексне вирішення зазначених проблем створить необхідні передумови для налагодження надійних та ефективних довірчих контактів, що сприятиме успішній протидії службовим правопорушенням у лавах Служби безпеки України.

Список використаних джерел:

1. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: Закон України від 23.12.1993 р. № 3782-XII: станом на 20 трав. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/3782–12#Text (дата звернення: 17.06.2024).

ПОНЯТІЙНИЙ ДИСБАЛАНС КОНТРРОЗВІДУВАЛЬНОЇ ТА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ

Володимир ГОРБ
співробітник СБУ

Оперативно-розшукова діяльність – це система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів [1].

Поняття контррозвідувальної діяльності міститься в чинному законі з однойменною назвою, що визначає її як спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України [2].

Аналіз поданих законодавцем притаманних оперативній роботі категорій оперативно-розшукової і контррозвідувальної діяльності визначень свідчить про їх перебування у певному протиріччі і неузгодженості. Адже наведена нижче блок-схема (Схема № 1) наочно демонструє, що зміст контррозвідувальної діяльності не тільки дублює оперативно-розшукову, а й значно ширше останньої.

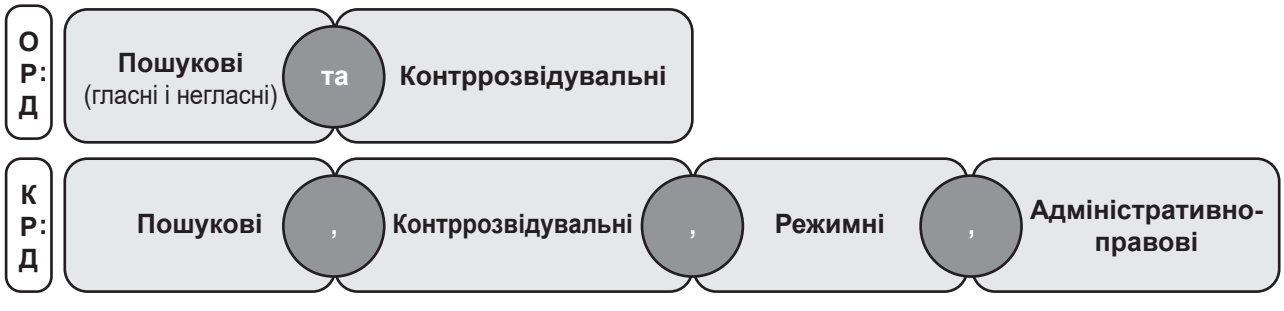


Схема № 1

Серед підстав для проведення оперативно-розшукової діяльності є наявність достатньої інформації за допомогою оперативно-розшукових заходів і засобів про 1) осіб, які готують вчинення кримінального правопорушення; 2) осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання; 3) осіб безвісно відсутніх; 4) кримінальні правопорушення, що готуються; 5) розвідувально-підривну діяльність спецслужб іноземних держав, організацій та окремих осіб.

На думку автора, для виконання перелічених завдань № 1, № 2, № 3, доречна така форма оперативно-розшукової діяльності як «оперативний розшук», тоді як для завдання № 5 – «оперативний пошук», а для № 4 – комплексне застосування обох форм. Їх включення у склад поняття ОРД дозволить уникнути існуючих нині колізій.

В той же час, існуюча логічна категорія контррозвідувальної діяльності, на погляд автора, також не досконала. Організаційні форми контррозвідувальної діяльності – це види контррозвідувальних дій, що відрізняються між собою цілями їх проведення, тривалістю, змістом. Цілі контррозвідки як і її мета, корелюються з завданнями, викладеними у статті 2 Закону України «Про контррозвідувальну діяльність»: попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення [2]. Зазначене обумовлює існування чотирьох провідних форм контррозвідувальної діяльності: контррозвідувальний пошук, забезпечення контррозвідувального режиму, контррозвідувальна перевірка чи розробка, активні контррозвідувальні заходи.

Методи контррозвідувальної діяльності це конкретні дії (оперативно-тактичні прийоми, заходи) оперативного складу, спрямовані на практичне вирішення завдань контррозвідки. Вони виступають як інструмент для отримання оперативно-вагомої інформації, вирішення практичних завдань, створення передумов чи бази для них відповідно до визначеної компетенції.

Тож пошукові заходи контррозвідника здійснюються у формі контррозвідувального пошуку, а режимні заходи (в т.ч. внутрішньооб'єктовий, перепускний режими, режим секретності, режими обмеження роботи радіозасобів тощо) реалізуються задля встановлення дієвого контррозвідувального режиму на об'єкті чи лінії роботи. Дискусійним є і питання відокремленості адміністративно-правових заходів, оскільки у разі проведення адміністративного впливу у вигляді притягнення особи до адміндповідальності за порушення законодавства у сфері державної таємниці такий захід є складовою забезпечення контррозвідувального режиму.

Викладені обставини обумовлюють авторське бачення формулювань оперативно-розшукової і контррозвідувальної діяльності:

Оперативно-розшукова діяльність – це система гласних і негласних антикримінальних заходів оперативного розшуку, пошуку, перевірки і розробки, що здійснюються із застосуванням оперативних та оперативно-технічних засобів.

Контррозвідувальна діяльність – це спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних форм і методів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувально-підривним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України.

Таке унормування дозволить виключити зіткнення поглядів науковців і практиків. Адже з одного боку, оперативні підрозділи Національної поліції уповноважені на проведення оперативно-розшукової діяльності, що складається з пошукових і контррозвідувальних заходів, а з іншого де-юре не можуть її проводити, оскільки відповідно до ст. 5 Закону України «Про контррозвідувальну діяльність» не являються суб'єктами її здійснення.

Список використаних джерел:

5. Закон України від 18 лютого 1992 року № 2135-XII «Про оперативно-розшукову діяльність». Редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2135–12#Text. (дата звернення 14.06.2024 р.)
6. Закон України від 26 грудня 2002 року № 374-IV «Про контррозвідувальну діяльність». Редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/374–15#Text. (дата звернення 14.06.2024 р.)

ОКРЕМІ ПИТАННЯ ВИКОРИСТАННЯ КОНФІДЕНЦІЙНИХ МОЖЛИВОСТЕЙ З МЕТОЮ ПРОТИДІЇ КОЛАБОРАЦІЙНІЙ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО АБО НАДЗВИЧАЙНОГО СТАНУ В УКРАЇНІ

В’ячеслав ГОРДІЄНКО
кандидат юридичних наук,
співробітник СБУ

Агресивна війна, яку розпочала російська федерація, є насущною проблемою для українського народу, яка поставила питання про основи соціального життя, людяності, колективної єдності, а також про життєздатність та ефективність мотивуючих сил європейської цивілізації. Опір агресії є результатом згуртованої волі всього українського народу, спрямованої на збереження соціальних демократичних цінностей. Завдання це є надзвичайно складним.

Визначення, адаптація, фіксація поточних (воєнних) змін та керування ними є однією з умов перемоги у війні. Кримінальна протиправність у вигляді колабораційної діяльності є важливим фактором, що впливає на перебіг і результати війни, враховуючи протиправну природу самої агресії та функціонування російського терористичного режиму. Тому результативна протидія колабораційній діяльності, поряд з ефективними діями в тилу та на полі бою, є взаємопов’язаними завданнями, хоча й потребують різних підходів для реалізації.

Аналіз наукової літератури, вивчення практичних результатів контррозвідувальної та оперативно-розшукової діяльності з використанням конфіденційних (негласних) можливостей оперативних підрозділів Служби безпеки України свідчать про недостатнє використання можливостей негласного апарату направленого на протидію колабораційній діяльності, проявам сепаратизму та проросійського реваншизму. Зазначене змушує стверджувати про наявність проблем використання конфіденційних можливостей під час контррозвідувальної та оперативно-розшукової протидії колабораційній діяльності в умовах воєнного або надзвичайного стану, яка на сьогодні досить актуальна та викликає чималий інтерес практиків та теоретиків. І для цього є певні причини:

– по-перше, одним із головних завдань оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах безпеки громадян, суспільства і держави [1], зокрема стосовно колабораційної діяльності в умовах воєнного стану;
– по-друге, одним із завдань контррозвідувальної діяльності є добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності організацій, окремих груп та осіб на шкоду державній безпеці України [2];

– по-третє, одним із основних способів отримання інформації про підготовку та вчинення кримінальних правопорушень, зокрема тих, що містять ознаки колабораційної діяльності є саме агентурно-оперативний метод, який оперативні підрозділи Служби безпеки України безпосередньо застосовують під час роботи з негласним апаратом.

Чинне законодавство у ст. 111–1 Кримінального кодексу України передбачає кримінальну відповідальність за колабораційну діяльність [3]. Враховуючи той факт, що зазначена норма є новою для вітчизняної правозастосовної практики, виникають окремі проблемні питання щодо контррозвідувальної та оперативно-розшукової протидії проявам колабораційної діяльності з використанням агентурно-оперативних можливостей [4].

Слід зазначити, що особливості об'єктивної сторони кримінального правопорушення, передбаченого ст. 111–1 КК України, є широкий перелік діянь, які охоплюються вказаним складом кримінального правопорушення, обумовлюють специфіку організації і тактики контррозвідувального та оперативно-розшукового документування протиправної діяльності колаборантів, перелік сил і засобів, які залучаються для виконання конкретних завдань [5].

Процес підбору та залучення осіб до конфіденційного співробітництва під час контррозвідувальної протидії колабораційній діяльності потребує вивчення, як безпосередньо організаційної сторони, так і попереднього аналізу певних ментальних та психологічних факторів кандидатів, які також необхідно враховувати в умовах сьогодення.

Залучення осіб до конфіденційного співробітництва має відповідати таким вимогам:

– цілеспрямованість залучення;
– добровільність конфіденційного співробітництва;
– доцільність залучення;
– безпека;
– надійність.

Розглядаючи організаційно-тактичні питання підвищення ефективності підбору та залучення осіб до конфіденційного співробітництва оперативними підрозділами Служби безпеки України під час контррозвідувальної діяльності направленої на протидію колабораційної діяльності, потрібно зупинитися на загальних нормативних вимогах та напрацьованих багатою практикою формах, дотримання яких вважається необхідним для такої діяльності.

Підбір та залучення оперативними підрозділами Служби безпеки України осіб до конфіденційного співробітництва розпочинається з аналітичної роботи щодо визначення необхідності залучення особи з певними характеристиками та можливостями у якості негласного джерела оперативної інформації (агента, негласного позаштатного працівника). Поряд з вивченням оперативної обстановки та визначенням необхідності вербування особи, вивчаються індивідуальні якості такого кандидата. Вимоги, яким повинен відповідати кандидат, визначають подальший характер відносин, що складаються у процесі конфіденційного співробітництва [6, с. 35]. Вивчення кандидата повинно спрямовуватися на з'ясування його реальної можливості та здатності виконувати завдання, які на нього планується покласти, особистісних якостей, ставлення до Служби безпеки України, ступеня відвертості перед оперативним співробітником та надійності, наявності обставин, що унеможливлюють конфіденційне співробітництво.

Як свідчить практичний досвід оперативних підрозділів Служби безпеки України під час контррозвідувальної чи оперативно-розшукової протидії колабораційній діяльності, надто складно підібрати особу, яка поєднує в собі весь комплекс необхідних особистих та ділових якостей. З метою ефективного здійснення особами, залученими до конфіденційного співробітництва, покладених на них завдань, проводиться їх навчання, яке складається з правової, спеціальної та психологічної підготовки. Навчання проводиться оперативним співробітником, зміст та обсяг такого навчання зумовлюється рівнем його фахової підготовки та обсягом виконання покладених на нього завдань.

Отже, змістом конфіденційного співробітництва під час контррозвідувальної, оперативно-розшукової протидії колабораційній діяльності в умовах воєнного стану є дії з добору, ви-

вчення, перевірки й залучення громадян до конфіденційного співробітництва; ефективна розстановки негласного апарату; їх використання у протидії колаборaційній діяльності; зв'язку та керівництва; правового і соціального захисту; матеріально-технічного забезпечення; формування резерву та процедури припинення конфіденційного співробітництва.

Підводячи підсумок, необхідно наголосити на тому, що з метою підвищення ефективності використання конфіденційних (негласних) можливостей під час контррозвідувальної, оперативно-розшукової протидії колаборaційній діяльності в умовах воєнного стану нами вбачається перспективність здійснення навчання негласного апарату можливостям кримінального профайлінгу. Ефективність використання негласним апаратом технології, яка поєднує методи вербальної та невербальної психодіагностики з метою профілювання для доказової бази або запобігання протиправним діям за допомогою виявлення потенційно небезпечних осіб і ситуацій з використанням методів прикладної психології, стане дієвим засобом на етапі виявлення первинної оперативно-розшукової інформації щодо підготовки та вчинення колаборaційних дій, її перевірки і реалізації шляхом створення психологічного портрета колаборантів, визначення протиправної поведінки таких осіб тощо.

Окремо підкреслимо, що, задіюючи негласний апарат з метою документування колаборaційної діяльності, варто мати на увазі те, що робота з агентурною мережею є лише засобом досягнення окремих (проміжних) результатів під час контррозвідувальної або оперативно-розшукової протидії колаборaційній діяльності в умовах воєнного стану, який не може розглядатись як самостійний показник діяльності оперативних підрозділів Служби безпеки України. Особливу увагу необхідно приділяти комплексному підходу з протидії кримінальній протиправності, покращенню якісного складу, а не збільшенню кількості негласного апарату.

Список використаних джерел:

1. Про оперативно-розшукову діяльність: закон України від 18.02.1992 № 2135-XII зі змін. URL: http: // https://zakon.rada.gov.ua/laws/show/2135–12#Text . (дата звернення 17.06.2024 р.)

2. Про контррозвідувальну діяльність: Закон України від 26 грудня 2002 року № 374-IV. Редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/374–15#Text . (дата звернення 17.06.2024 р.)

3. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колаборaційну діяльність: Закон України від 03.03.2022 р. № 2108-IX. URL: https://zakon.rada.gov.ua/laws/show/2108–20/print . (дата звернення 17.06.2024 р.)

4. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. // Верховна Рада України. Офіційний вебпортал парламенту України. [Електронний ресурс]. URL: https:// https://zakon.rada.gov.ua/laws/show/2341–14#Text. (дата звернення 17.06.2024 р.)

5. Кримінальний кодекс України. Науково-практичний коментар. Станом на 25 квітня 2024 року. / За заг. ред. Копотуна І.М.– Київ: Вид. «Центр учбової літератури», 2024. 1352 с.

6. Гусаров С.М. Генезис запровадження негласних слідчих (розшукових) дій у законодавство та практичну діяльність правоохоронних органів України. Європейські перспективи, 2013. № 3. С. 35–39.

ТАКТИКА ПРОТИДІЇ ФІНАНСУВАННЮ ТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ, ЯК ОКРЕМИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Адам ДАЛЬ
кандидат юридичних наук,
старший науковий співробітник
Національного юридичного
університету імені Ярослава Мудрого

Тероризм є сучасною глобальною загрозою людству, що характеризується найвищим ступенем суспільної небезпеки. Домінуючою у міжнародному співтоваристві є точка зору, згідно з якою протидія терористичній діяльності не зводиться виключно до виявлення та припинення вчинення окремих кримінальних правопорушень терористичної спрямованості, а розглядається у більш широкому аспекті – з акцентуванням уваги на фінансову основу тероризму, яка відіграє важливу роль у породженні та існуванні цього антисуспільного явища. Дійсно, фінансова складова дає можливість тероризму, його людським, технічним, технологічним, науковим та іншими ресурсам організовуватися, відтворюватися та нарощувати силу.

Фінансові ресурси є необхідними для вербування нових учасників терористичних об'єднань, розробки та удосконалення нових технічних засобів здійснення терористичної діяльності, забезпечення підтримки населення як на території ведення такої кримінально-протиправної діяльності, так і за кордоном. Значні гроші витрачаються на пошук прихильників, бойову підготовку учасників терористичних об'єднань, створення центрів підготовки, покращення матеріально-технічної бази (придбання приміщень, військової техніки, засобів зв'язку, обчислювальної та комп'ютерної техніки, зброї, розробку нових схем та засобів отримання доходів тощо). У багатьох випадках характерними ознаками сучасної терористичної діяльності є стійкість із чіткою зорганізованістю та здатністю до модернізації, а також повним або частковим самофінансуванням.

Особливе значення для боротьби з тероризмом має Міжнародна конвенція «Про боротьбу з фінансуванням тероризму», що була прийнята Резолюцією 54/109 Генеральної Асамблеї ООН від 9 грудня 1999 р. [1] та ратифікована Законом України «Про ратифікацію Міжнародної конвенції про боротьбу з фінансуванням тероризму» від 12 вересня 2002 р. № 149-IV [2].

З метою імплементації в національне кримінальне законодавство положень вказаної Конвенції у Кримінальному кодексі України в редакції від 18 травня 2010 р. було додано статтю 258–5 («Фінансування тероризму») [3].

Об'єктом фінансування тероризму є громадська безпека як різновид національної безпеки України. Особливістю громадської безпеки як об'єкта цього кримінального правопорушення є те, що виникає і/або існує джерело підвищеної небезпеки для суспільства – у даному випадку у вигляді забезпечувального чинника терористичної діяльності, яким є її фінансове або інше забезпечення з фінансовим складником [4].

Сучасна складна оперативна обстановка у сфері забезпечення державної безпеки вимагає від СБ України нейтралізації сучасних загроз, що безпосередньо залежить від вибору ефективного та раціонального способу здійснення зазначеного, обрання адекватної, вирішенню поставлених завдань та оперативної обстановки, послідовності дій. Зазначене безпосередньо стосується і протидії фінансуванню тероризму оперативними підрозділами СБ України, що зумовлює дослідження тактики здійснення такої діяльності. Адже, результатом вчинення сус-

пільно небезпечних діянь, передбачених ст. 258–5 КК України, буде організація, підготовка або вчинення терористичного акту, втягнення у вчинення терористичного акту, публічних закликів до вчинення терористичного акту, створення терористичної групи (організації), сприяння вчиненню терористичного акту, навчання тероризму, перетинання державного кордону України з терористичною метою, провадження будь-якої іншої терористичної діяльності тощо. Оборудки таких матеріальних активів становить пряму загрозу державній безпеці України [3].

Тактика протидії СБ України фінансуванню тероризму, в загальному її розумінні є поєднанням теорії та практики використання найбільш ефективних форм, способів та методів реалізації зазначеного. Теоретична складова тактики протидії СБ України фінансуванню тероризму, має забезпечувати вивчення закономірностей, принципів, характеру та змісту такої діяльності оперативних підрозділів СБ України. При цьому наукові дослідження тактики протидії фінансуванню тероризму, мають спрямовуватись на вивчення прийомів, способів, форм діяльності оперативних підрозділів СБ України у різних умовах оперативної обстановки, методів вирішення поставлених завдань, нестандартних підходів до використання оперативних сил та засобів. Практична складова тактики протидії СБ України фінансуванню тероризму, має полягати у найбільш дієвому застосуванні оперативними підрозділами СБ України теоретичних положень і принципів тактики організації та здійснення виявлення ознак діяльності, пов'язаної із фінансуванням тероризму та запобігання використання фінансових активів у терористичної діяльності. Результатом тактики СБ України з протидії фінансуванню тероризму, як практичної складової, слід вважати ефективне використання наявних оперативних сил, засобів та методів контррозвідувальної та оперативно-розшукової діяльності з урахуванням поточної оперативної обстановки, що забезпечує ефективне вирішення виконання завдань, покладених на службу безпеки.

При цьому тактика діяльності СБ України із протидії фінансуванню тероризму, може існувати як категорія науки та практики на різних рівнях вирішення завдань із забезпечення державної безпеки України. Так, ураховуючи поточну політичну, економічну, соціальну обстановку в державі, СБ України, зважаючи на реальні та потенційні загрози, виробляються загальні тактичні настанови, обов'язкові для урахування при плануванні, організації та проведенні операцій, заходів, дій оперативних підрозділів СБ України на усіх без виключення лініях, напрямах забезпечення державної безпеки. Окреслені питання є прерогативою тактики діяльності СБ України із протидії фінансування тероризму.

Формування тактики діяльності СБ України з протидії фінансуванню тероризму, може розглядатись як процес прийняття рішення щодо найбільш ефективного способу вирішення завдань із реалізації зазначеного. Водночас, слід наголосити на тому, що ефективність вирішення завдань із забезпечення державної безпеки залежить від якості прийнятого рішення, вибору оптимального способу дій для досягнення визначеної мети, наукової обґрунтованості, компетентності та своєчасності.

Ураховуючи викладене, під тактикою протидії СБ України фінансуванню тероризму, можна розуміти вироблену теорією та підтверджену практикою раціональну та ефективну послідовність дій оперативних підрозділів, спрямованих на своєчасне виявлення, попередження та припинення фінансової операції чи правочину з коштами або іншими матеріальними активами, у тому числі, що одержані кримінально протиправним шляхом та недопущення їх використання у фінансуванні тероризму, з урахуванням особливостей оперативної обстановки та характеру реальних і потенційних загроз.

Аналіз матеріалів практики діяльності СБ України дає підстави визначити наступні характеризуючі ознаки тактики протидії фінансуванню тероризму, до яких можна віднести:

1. підпорядкованість стратегічним засадам політики держави у сфері забезпечення державної безпеки, а саме: виявлення, попередження, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління, економіки та інших протиправних дій, що безпосередньо створюють загрозу життєво важливим інтересам України, які віднесено до завдань СБ України;

2. спрямованість на виявлення на ранніх стадіях ознак підготовки до вчинення фінансової операції чи правочину з коштами або іншими матеріальними активами, пов'язаними з терористичною діяльністю, недопущення їхнього використання у фінансуванні тероризму;

3. централізація та уніфікація тактичних прийомів оперативних підрозділів СБ України пов'язаних з протидією фінансуванню тероризму;

4. адаптивність тактичних прийомів та методів оперативних підрозділів СБ України до змін в кримінально протиправному середовищі, своєчасне реагуванням на тенденції розвитку оперативної обстановки пов'язаної з фінансуванням тероризму;

5. спрямованість на виявлення та усунення причин та умов, що сприяють виникненню реальних та потенційних загроз державній безпеці України, джерелом яких є терористична діяльність та її фінансування.

Список використаних джерел:

1. Міжнародна конвенція про боротьбу з фінансуванням тероризму (укр/рос). Конвенція, Міжнародний документ від 09.12.1999. [Електронний ресурс] URL: https://zakon.rada.gov.ua/laws/show/995_518#Text . (дата звернення 19.06.2024 р.)

2. Про ратифікацію Міжнародної конвенції про боротьбу з фінансуванням тероризму: Закон України від 12.09.2002 № 149-IV. Верховна Рада України. Офіційний вебпортал парламенту України. [Електронний ресурс]. URL: Електронний ресурс: https://zakon.rada.gov.ua/laws/show/149–15#Text . (дата звернення 19.06.2024 р.)

3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. // Верховна Рада України. Офіційний вебпортал парламенту України. [Електронний ресурс]. URL: https:// https://zakon.rada.gov.ua/laws/show/2341–14#Text . (дата звернення 19.06.2024 р.)

4. Кримінальний кодекс України. Науково-практичний коментар. Станом на 25 квітня 2024 року. / За заг. ред. Копотуна І.М.– Київ: Вид. «Центр учбової літератури», 2024. 1352 с.

ЩОДО РОЗРОБКИ КОНЦЕПЦІЇ РОЗВИТКУ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Валерій ДАРАГАН
доктор юридичних наук, професор,
завідувач кафедри
оперативно-розшукової діяльності
Дніпровського державного
університету внутрішніх справ

На сьогодні в Україні триває процес реформування органів внутрішніх справ та правоохоронної системи у цілому, вплив як зовнішніх, так і внутрішніх факторів зумовлює необхідність постійного удосконалення нормативно-правового забезпечення діяльності підрозділів Національної поліції, зміни їх структурно-функціональної побудови, а це визначає потребу своєчасного наукового аналізу та розробок з метою їх впровадження у практичну діяльність, а також удосконалення якості підготовки відповідних фахівців [1].

Вирішення проблем оперативно-розшукової діяльності підрозділів Національної поліції України можливе лише за наявності відповідної стратегії, котра має виражатися у нормативно-правових актах, спрямованих на забезпечення вирішення завдань оперативно-розшукової діяльності. Стратегія як спосіб дій є необхідною в ситуації, коли для прямого досягнення осно-

вної мети недостатньо наявних ресурсів. Завданням стратегії є ефективне використання наявних ресурсів для досягнення основної мети. Стратегію дій визначає концепція (доктрина), тобто комплекс поглядів, які пов'язані між собою та випливають один з одного, система шляхів вирішення обраного завдання [2, с. 424–425].

Підрозділи кримінальної поліції є одним з основних суб'єктів реалізації оперативно-розшукової функції серед органів та підрозділів Національної поліції України. Від результатів діяльності вказаних підрозділів залежить стан розкриття більшості неочевидних кримінальних правопорушень, забезпечення проведення більшості негласних слідчих (розшукових) дій за кримінальними провадженнями, підслідними органам досудового розслідування Національної поліції, а також превенція кримінальних правопорушень, що готуються [3].

На сьогодні в системі реалізації оперативно-розшукової функції Національної поліції України накопичилось чимало проблем як у нормативному так і у структурно-функціональному забезпеченні, які потребують вирішення.

Аналіз діяльності оперативних підрозділів Національної поліції України показав, що на сьогодні існують окремі проблеми, які не дозволяють якісно реалізовувати оперативно-розшукові функції. Зокрема, до таких проблем ми відносимо такі:

– прорахунки у підготовці фахівців для підрозділів кримінальної поліції;
– прорахунки у структурній побудові окремих підрозділів кримінальної поліції;
– прорахунки у розподілі функцій між підрозділами кримінальної поліції;
– прогалини нормативного забезпечення діяльності підрозділів кримінальної поліції.

В основу професійної діяльності підрозділів кримінальної поліції Національної поліції України покладено виконання ними оперативно-розшукової функції. Тому саме на отримання відповідних знань, умінь та навичок повинна бути спрямована й система їх підготовки [4].

На сьогодні підготовка фахівців для підрозділів кримінальної поліції в закладах вищої освіти МВС України здійснюється відповідно до типового навчального плану «Правоохоронна діяльність (поліцейські)» першого (бакалаврського) рівня вищої освіти за спеціальністю 262 Правоохоронні діяльність.

Основу професійної компоненти відповідної освітньої програми складають комплекси навчальних дисциплін серед яких й «Оперативно-розшукова діяльність». Крім того, серед дисциплін спеціалізації (вибіркові дисципліни) присутні й такі як: «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції»; «Використання кримінального аналізу підрозділами кримінальної поліції»; «Взаємодія підрозділів кримінальної поліції з іншими підрозділами НПУ»; «Міжнародне співробітництво в оперативно-розшуковій діяльності»; «Оперативно-розшукове документування»; «Негласні-розшукові дії»; «Агентурно-оперативна робота»; «Оперативно-розшукова тактика»; «Проведення оперативно-розшукових заходів підрозділами кримінальної поліції»; «Розшукова робота підрозділів кримінальної поліції»; «Використання оперативної техніки підрозділами кримінальної поліції», «Розкриття окремих видів злочині». Комплекс зазначених дисциплін надає змогу отримати здобувачам вищої освіти необхідні для майбутньої професійної діяльності знання, уміння та навички. Однак слід констатувати, що на сьогодні існує ряд проблемних питань, які негативно впливають на якість такої підготовки.

По-перше, враховуючи те, що вивчення переважної більшості вище зазначених навчальних дисциплін передбачає роботу з джерелами інформації, які мають гриф обмеженого доступу «Для службового користування» або гриф секретності «Таємно» їх вивчення здійснюється у спеціально обладнаних для цього приміщеннях. Однак, у разі оголошення повітряної тривоги, відповідно до діючих інструкцій, навчальна група разом з науково-педагогічним працівником повинна перейти в укриття. При цьому відповідних обладнаних аудиторій в приміщенні укриття немає, а тому вивчення відповідної дисципліни в таких умовах продовжуватися не може. Звісно науково-педагогічний працівник надає відповідні завдання на самостійну підготовку, однак вона жодним чином не може замінити роботу в аудиторії, тим паче у випадку коли проведення таких занять у активній формі або у формі поліцейського квесту з максимальною імі-

тацією до умов роботи у практичному підрозділі. Крім того, здобувачі вищої освіти не завжди мають достатню кількість часу на додаткову самостійну підготовку оскільки більшість з них приймає активну участь у громадській та волонтерській діяльності. Вказане негативно впливає на якість отриманих знань, умінь та навичок.

По-друге, в окремих закладах вищої освіти МВС України на сьогодні спостерігається проблема з недостатньою кількістю навчальної та наукової літератури у спеціальних бібліотеках (здебільшого з грифом секретності) оскільки на початку незаконного вторгнення російської федерації на нашу територію, окремі заклади вищої освіти були змушені знищити відповідні носії інформації, оскільки вони становили державну таємницю. Якщо з навчальною літературою ситуація з кожним роком поліпшується, то з науковою літературою значно складніше, оскільки не кожен вчений готовий та має можливість перевипустити свою наукову продукцію. Тому на сьогодні, в окремих випадках, є проблеми в реалізації не тільки освітньої компоненти, а й наукової.

На сьогодні триває процес реформування ОВС у частині оптимізації структури Національної поліції, чіткого розмежування та усунення дублювання їх повноважень, а також позбавлення підрозділів органів Національної поліції невластивих їм функцій. До основних напрямів реформування слід віднести такі:

– розмежування компетенції та функцій, усунення дублювання в роботі;
– оптимізація структури Національної поліції та чисельності;
– впровадження нових критеріїв оцінки роботи працівників органів та підрозділів Національної поліції; переатестація особового складу з метою підвищення якості кадрового забезпечення правоохоронної діяльності [5, с. 255–256].

На початку 2021 року керівництвом МВС України та Головою Національної поліції України презентовано нову модель організації діяльності Національної поліції України [6], яка вже втілена у життя. Насамперед, такі зміни обумовлені проведенням в Україні адміністративно-територіальної реформи та реалізації принципу децентралізації державної влади, в результаті чого 490 районів було ліквідовано, натомість створено 119 і 17 на тимчасово окупованих територіях. Також на шляху до подальшого розвитку Національної поліції України обрано побудову її організаційної структури та засад функціонування відповідно до міжнародних стандартів з метою вдосконалення управлінських процесів, а також діяльності з надання поліцейських послуг громадянам в правоохоронній сфері [7, с. 34].

Відштовхуючись від цих нововведень та з урахуванням новоутворених районів на території нашої держави з'явилося підрозділи поліції – управління та відділи. З метою максимального охоплення усього населення поліцейським захистом, у їх складі створені відділи, відділення та сектори поліцейської діяльності. Слід визнати, що така структурна побудова поліції має певні недоліки, насамперед на рівні місцевих управлінь Національної поліції. Це призводить до скорочення підрозділів прямого підпорядкування, та створює труднощі у координації здійснення забезпечення публічної безпеки та порядку на певній території [8, с. 31].

У той же час відділення поліції поділені на два типи: одні у своєму штаті мають слідчі підрозділи та карний розшук, а в інших залишилися лише дізнання та превентивні служби. Це пояснюється тим, що злочини невеликої тяжкості тепер є кримінальними проступками, які можуть розслідувати поліцейські офіцери громади, дільничні та працівники ювенальної превенції. Відповідно, не всі невеликі підрозділи потребують у своїй структурі кримінальну поліцію та слідство, включаючи ту обставину, що населення на окремих територіях обслуговування в принципі малочисельне, а криміногенна ситуація спокійна. При цьому сектори поліцейської діяльності – це невеликі підрозділи поліції, в яких функціонує лише превенція – тобто групи реагування, які оперативно виїжджають на виклики за номером 102, а також дільничні офіцери поліції, які безпосередньо працюють із населенням [7, с. 35].

Однак відсутність в окремих територіальних одиницях працівників кримінальної поліції унеможливлює якісного виконання ними оперативно-розшукової функції.

Аналіз функцій підрозділів кримінальної поліції показав, що лише незначна кількість функцій таких підрозділів направлена на виконання оперативно-розшукової функції Націо-

нальної поліції. Крім того, окремі із вказаних функцій не направлені на виконання завдань оперативно-розшукової діяльності, а лише сприяють їх виконанню. Відповідна ситуація складається й нормативному забезпечення компетенції кримінальної поліції щодо виконання оперативно-розшукових функцій. У деяких підрозділах на нормативному рівні не закріплені їх права взагалі (підрозділи Департаменту карного розшуку; Департамент забезпечення діяльності, пов'язаної з небезпечними матеріалами) хоча вказані підрозділи приймають безпосередню участь у виявленні та оперативно-розшуковому документуванні кримінальних правопорушень [9; 10].

Крім того, на сьогодні важливим напрямком розробки концепції розвитку оперативно-розшукової діяльності підрозділів Національної поліції України є формування механізмів, направлених реалізацію оперативно-розшукової функції у післявоєнний період.

Вказаному питання необхідно приділити значну частину вказаної концепції адже у після воєнний період правоохоронна система, без відповідної її стратегії розвитку та утримання у працездатному стані, з великою вірогідністю зазнаватиме великих проблем, у першу чергу пов'язаних з якісним кадровим потенціалом.

Вказані проблеми будуть зумовлені багатьма факторами, зокрема:

– значна кількість оперативних працівників одразу майже одразу після закінчення війни, з великою вірогідністю, підуть на пенсію;
– у зв'язку з зупинкою здійснення надання додаткової винагороди поліцейським під час дії воєнного стану, відсутності дієвих механізмів соціальної підтримки та значним навантаженням у післявоєнний період, окремі молоді фахівці будуть звільнятися з органів Національної поліції України;
– приватний сектор, який у після воєнний період буде мати значні проблеми з кадровим забезпеченням в окремих професіях, які як правило займали особи чоловічої статті буде змушений створювати умови задля заповнення відповідних вакансій, у тому числі за рахунок пошуку таких працівників серед діючих працівників поліції.

Враховуючи вище вказане, основними напрямками розробки Концепції розвитку оперативно-розшукової діяльності підрозділів Національної поліції України пропонується визначити:

– вдосконалення системи управління підрозділами кримінальної поліції Національної поліції України;
– удосконалення структурно-функціонального забезпечення діяльності підрозділів кримінальної поліції Національної поліції України;
– реформування національного законодавства з питань оперативно-розшукової діяльності шляхом прийняття нового закону «Про оперативно-розшукову діяльність»;
– удосконалення системи відомчого нормативного забезпечення виконання оперативно-розшукових функцій підрозділами Національної поліції України;
– забезпечення систематичної підготовки фахівців для підрозділів кримінальної поліції Національної поліції України;
– розробка та впровадження електронних депозитаріїв для навчальної та наукової літератури з грифом секретності або обмеження доступу;
– впровадження механізмів соціального захисту працівників оперативних підрозділів Національної поліції України.

Список використаних джерел:

1. Кобзар О.Ф., Дараган В.В. Напрямки удосконалення підготовки фахівців для органів досудового розслідування Національної поліції. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. № 1. С. 158–163.

2. Кириченко О.В. Методологічні підходи дослідження проблем оперативно-розшукової протидії злочинам проти громадської безпеки. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2013. № 3. С. 421–427.

3. Дараган В.В., Карповський С.В., Копилов Е.В. Стан та перспективи розвитку підготовки фахівців для підрозділів кримінальної поліції та органів досудового розслідування у закладах вищої освіти МВС України. Scientific monograph. Academic Council of Baltic ResearchInstitute of Transformation Economic Area Problems according to the Minutes № 4 dated 2023. С. 40–53.

4. Дараган В.В. Деякі проблеми підготовки фахівців для підрозділів кримінальної поліції закладами вищої освіти в умовах війни. Законодавчі аспекти протидії особливо небезпечним злочинам в Україні. Матеріали міжнародного науково-практичного круглого столу 14–15 березня 2024 року, м. Київ. Київ: Алерта, 2024. С. 25–28.

5. Кириченко О.В. Кримінальна поліція як суб'єкт оперативно-розшукової протидії злочинам проти громадської безпеки. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2015. № 4. С. 254–260.

6. Ігор Клименко презентував нову модель організації діяльності Національної поліції України. Урядовий портал: офіц. сайт. 11.11.2023. URL: https://www.kmu.gov.ua/news/igor-klimenkoprezentuvav-novu-model-organizaciyi-diyalnosti-nacionalnoyi-policiyiukrayini. (дата звернення 19.06.2024 р.)

7. Гусаров С.М. сучасний стан побудови організаційної структури Національної поліції України. Проблеми сучасної поліцеїстики: тези доп. наук.– практ. конф. (м. Харків, 20 квіт. 2022 р.) / МВС України, Харків. нац. ун-т внут. справ. Харків: ХНУВС, 2022. С. 32–36.

8. Гусаров С.М. Деякі питання оптимізації структури Національної поліції України. Наше право. 2017. № 1. С. 27–32.

9. Огурченко В.Г., Рогальська В.В. Нормативно-правове забезпечення оперативно-розшукової функції Національної поліції України: проблеми та шляхи їх вирішення. Науковий вісник Дніпропетровського державного університету внутрішніх справ. Науковий журнал. 2022. Спеціальний випуск. С. 31–40.

10. Огурченко В.Г., Рогальська В.В. Щодо визначення функцій оперативних підрозділів Національної поліції як суб'єктів виконання оперативно-розшукової функції. Науковий вісник Дніпропетровського державного університету внутрішніх справ. Науковий журнал. 2023. Спеціальний випуск. С. 34–39.

НАПРЯМИ ВИКОРИСТАННЯ ГЕНЕРАТИВНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ В РАМКАХ КОНТРРОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ ОРГАНІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Дмитро ЗОРЕНКО
доцент Національного юридичного
університету імені Ярослава Мудрого

Відповідно до положень ст. 2 Закону України «Про контррозвідувальну діяльність» ключовими завданнями контррозвідувальної діяльності є добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, організацій, окремих груп та осіб на шкоду державній безпеці України, а також розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян (курсів – авт.) [1].

Генеративний штучний інтелект (далі – ШІ) привернув увагу світової громадськості наприкінці 2022 р. з презентацією ChatGPT, що став першим широкодоступним та простим у використанні чат-ботом на його основі. Подібні інструменти здатні імітувати можливості людини по створенню різноформатного контенту (текстів, зображень, відео, музики, програмного коду),

слугувати засобом пошуку інформації та розширення знань, аналізувати великі обсяги даних, здійснювати переклад чи транскрибацію мультимедійного контенту тощо. Сьогодні мільйони людей регулярно користуються ними в повсякденному житті й потенціал адаптації конкретних моделей ШІ до специфічних сфер застосування видається практично необмеженим.

Так, у 2024 р. американське розвідувальне співтовариство, визнаючи критичну важливість і постійно зростаючий обсяг матеріалів розвідки з відкритих джерел (OSINT) у своїй діяльності, розпочало впровадження нової стратегічної ініціативи, спрямованої на суттєве покращення процедур збору, опрацювання та формування результатів OSINT, розраховану на період до 2026 р. Центральне місце в ній посідає проблематика застосування технологій ШІ та машинного навчання, що розглядаються в якості інноваційних інструментів роботи з відкритими даними та потенційно здатні підвищити ефективність і точність OSINT-досліджень за рахунок автоматизації виявлення й аналізу релевантної інформації з величезної кількості загальнодоступних даних. Однак, у цій стратегії також визнаються проблеми, пов'язані із забезпеченням достатності та достовірності отриманих в такий спосіб відомостей, акцентується увага на важливості впровадження ефективних протоколів їх перевірки [2].

На даний час для добування інформації контррозвідувального характеру краще підходять багатофункціональні комерційні моделі генеративного ШІ, приміром ChatGPT, Claude, Gemini, Copilot, Perplexity, You, що можуть бути використані з метою:

- цілеспрямованого пошуку та збору відомостей з веб-сайтів (приміром, новини, профілі та публікації в соціальних мережах, форуми, публічні реєстри й бази даних);
- формулювання ключових слів, ідей або переліку ресурсів, здатних розширити пошук, синтаксису пошукових операторів Google Dork чи соцмережі X (Twitter) для оптимізації кінцевої видачі, а також команд профільних Github-утиліт;
- написання та/або оптимізації коду скриптів для парсингу (автоматизованого збору) даних, моніторингу інтернет-ресурсів, виконання інших періодичних пошукових завдань;
- перекладу, транскрибації відео- та аудіоконтенту, обробки неструктурованих даних, їх систематизації (наприклад, згадки про людей, організації, події або місця, статистика, посилання) тощо.

Як відомо, доступ до зазначених онлайн-сервісів дуже простий – достатньо мати підключення до мережі «Інтернет», зручний браузер та пройти процедуру реєстрації. Однак, подібний підхід може стати підставою для появи побоювань за конфіденційність і безпеку даних користувача – фірми-розробники ШІ зберігають всю історію запитів, завантажені файли, метадані та інші відомості для подальшого навчання своїх продуктів. До того ж, комерційний (закритий) характер цих моделей встановлює заборону на можливість вивчення всіма зацікавленими особливостей їх архітектури, технічних параметрів, механізму розширення функціональних можливостей та кастомізації.

Для вирішення завдань контррозвідувальної діяльності, що пов'язані з певними обмеженнями у відкритому доступі до інформації, відмовлятися від ШІ зовсім не обов'язково – потрібно лише перенести обробку даних з хмарного середовища на спеціальний сервер, персональний комп'ютер чи навіть потужний ноутбук. Звісно, запустити власну версію Perplexity або Midjourney без доступу до інтернету навряд чи вдасться. Але, використовуючи інші безкоштовні генеративні моделі (приміром, LLaMA, Mistral, Command-R чи Phi), що мають відкритий вихідний код та працюють локально, можна отримати таку ж якість результатів, яка ще рік тому експертам здавалася еталонною.

Як і будь-де, існують переваги та недоліки подібних рішень.

До перших слід віднести їх здатність функціонувати на контрольованому з боку користувача сервері, що суттєво зменшує ризики витоку інформації або несанкціонованого доступу до неї. Високошвидкісна та захищена передача пакетів даних між абонентами реалізується за допомогою корпоративної оптоволоконної мережі незалежно від наявності інтернет-з'єднання.

Також, це підтримка повного доступу до налаштування, оптимізації та постійного навчання обраної моделі з метою її персоналізації для виконання прикладних завдань контррозвідуваль-

ної діяльності, задоволення існуючих та перспективних потреб специфічних споживачів продукту. Приміром, це може бути створення єдиної відомчої бази даних з можливістю отримання додаткових чи довідкових відомостей; формулювання контекстнозалежних алгоритмів оцінки здобутої інформації, її подальшої перевірки та документування фактів можливої протиправної діяльності; аналіз відомостей (виявлення тенденцій, настроїв, загроз, закономірностей чи взаємозв'язків, формулювання висновків і прогнозів) та підготовка проектів підсумкових документів, їх візуалізація (графіки, таблиці, діаграми, карти, схеми); оптимізація повторюваних процесів, в т.ч. елементів управлінського циклу (планування, прийняття рішень та організація їх виконання, звітність, контроль); нормотворчість та ін.

В якості других необхідно назвати залежність швидкості роботи цих моделей ШІ від доступних їм ресурсів центрального процесору, оперативної пам'яті, відеоадаптеру та дискової підсистеми. Пріоритетною мовою для більшості з них є англійська. Відповіді іншими мовами можуть бути недостатньої якості та містити помилки через незбалансованість бази даних, що використовується за замовчанням. Хоча багатомовні моделі частково або повністю позбавлені цього недоліку, але комфортна робота з ними неодмінно потребуватиме додаткового навчання та налаштування.

Підсумовуючи викладене, хотілося б наголосити на тому, що на сьогодні генеративний ШІ є одним з найпопулярніших напрямків розвитку цифрових технологій, можливості якого потенційно можуть бути використані в рамках вирішення широкого спектру завдань контррозвідувальної діяльності органів СБ України. В залежності від їх специфіки це може бути реалізовано на базі як комерційних онлайн-моделей, так і локальних рішень з відкритим вихідним кодом, що належним чином кастомізовані. Безумовно, кожна з них має свої особливості та обмеження, але те, що поява генеративних open source моделей ШІ істотно знизила поріг входу в світ нейромереж,– це вже факт.

Список використаних джерел:

1. Про контррозвідувальну діяльність: Закон України від 26.12.2002 № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374–15 (дата звернення: 20.06.2024).

2. The IC OSINT Strategy 2024–2026: веб-сайт. URL: https://s3.documentcloud.org/documents/24475002/ic_osint_strategy.pdf (дата звернення: 20.06.2024).

ДО ПИТАННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА РОЗГОЛОШЕННЯ ДАНИХ КОНТРРОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ

Олег ПЛЕТНЬОВ
кандидат юридичних наук, доцент,
завідувач кафедри Національного юридичного
університету імені Ярослава Мудрого
Євгеній КОВАЛЕНКО
кандидат юридичних наук, доцент,
професор Національного юридичного
університету імені Ярослава Мудрого

Наша країна долає складний шлях демократичних перетворень задля впровадження стандартів Європейської спільноти, що регулюють відносини між державними інститутами та людиною в ході забезпечення державної безпеки та боротьби зі злочинністю. З одного боку держава, в особі її правоохоронних органів та спеціальних служб, виконує функцію захисту громадян від зовнішніх та внутрішніх загроз (розвідувально-підривна діяльність, тероризм

та інші протиправні посягання) використовуючи при цьому конституційно закріплену виключну можливість здійснювати заходи, пов'язані з обмеженням прав і свобод людини і громадянина. В той же час людина має бути впевнена у всебічному забезпеченню реалізації своїх невід'ємних прав і свобод та захисті свого особистого життя, честі та гідності.

Наразі, питання гарантій дотримання законності під час здійснення контррозвідувальної діяльності (далі – КРД), оперативно-розшукової діяльності (далі – ОРД) та досудового розслідування висвітлено в Законі України «Про контррозвідувальну діяльність», Законі України «Про оперативно-розшукову діяльність» та в Кримінальному кодексі України відповідно. Втім, механізм притягнення до відповідальності за розголошення відомостей що стосуються особистого життя, честі та гідності людини, на нашу думку, є недосконалим, оскільки поза увагою законодавця залишились питання кримінальної відповідальності за вказані дії, якщо вони були вчинені саме у процесі здійснення КРД.

Вважаємо, що цей механізм є однією з важливих умов забезпечення гарантій законності тимчасового обмеження прав і свобод людини в ході проведення негласних заходів. Тому з'ясування та систематизація матеріально-правових і процесуально-правових гарантій прав і свобод людини під час здійснення КРД та ОРД дозволить виробити пропозиції щодо внесення відповідних змін до кримінального законодавства України.

Проведення негласних заходів, зокрема тих, що передбачають тимчасове втручання у приватне спілкування в КРД, ОРД та досудовому розслідуванні з організаційної та технічної точки зору схожі (підстави, отримання дозволу суду, строки, суб'єкти здійснення, засоби тощо). Вимоги до правоохоронних органів і спецслужб щодо законності проведення таких заходів також чітко визначені у законодавстві. За таких умов не зрозуміло, чому кримінальна відповідальність за порушення законодавства щодо розголошення відомостей ОРД та досудового розслідування зазначена у кримінальному законі, а за розголошення даних КРД, розкриття та оприлюднення яких можуть завдати суттєвої (а іноді і невиправної) шкоди державній безпеці України – будь-яка відповідальність у Кримінальному кодексі України не передбачається.

Так, у ст. 387 КК України «Розголошення даних оперативно-розшукової діяльності, досудового розслідування» передбачена кримінальна відповідальність за розголошення без дозволу прокурора, слідчого або особи, яка провадила ОРД, даних ОРД або досудового розслідування особою, попередженою в установленому законом порядку про обов'язок не розголошувати такі дані, а також за розголошення даних ОРД, досудового розслідування, вчинене суддею, прокурором, слідчим, працівником оперативно-розшукового органу незалежно від того, чи приймала ця особа безпосередню участь в ОРД, досудовому розслідуванні, якщо розголошені дані ганьблять людину, принижують її честь і гідність [1].

Водночас, не є кримінально караними такі дії, як оприлюднення або надання (розголошення) зібраних відомостей, а також інформації щодо проведення або непроведення стосовно певної особи контррозвідувальної діяльності та заходів до прийняття рішення за результатами такої діяльності або заходів (ст. 9 Закону України «Про контррозвідувальну діяльність»); розголошення інформації, що стосується особистого життя, честі та гідності людини, яка стала відома у процесі контррозвідувальної діяльності (ст. 11 Закону України «Про контррозвідувальну діяльність») [2].

На наш погляд, з урахуванням невідворотності процесу реформування Служби безпеки України у напрямку відповідності стандартам НАТО та ЄС, закріплення за нею суто контррозвідувальних функцій, а відтак і посилення гарантій забезпечення прав і свобод людини під час здійснення КРД, необхідно закріпити кримінальну відповідальність за діяння, що пов'язані із розголошенням даних КРД.

На нашу думку, доцільно внести відповідні зміни до статті 387 Кримінального кодексу України та викласти її у наступній редакції:

«Стаття 387. Розголошення даних контррозвідувальної або оперативно-розшукової діяльності, досудового розслідування.

1. Розголошення без письмового дозволу прокурора, слідчого або особи, яка провадила контррозвідувальну або оперативно-розшукову діяльність, даних контррозвідувальної або

оперативно-розшукової діяльності або досудового розслідування особою, попередженою в установленому законом порядку про обов'язок не розголошувати такі дані,–

карається штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або пробаційним наглядом на строк до двох років.

2. Розголошення даних контррозвідувальної або оперативно-розшукової діяльності, досудового розслідування, вчинене суддею, прокурором, слідчим, дізнавачем, працівником контррозвідувального або оперативно-розшукового органу незалежно від того, чи приймала ця особа безпосередню участь в контррозвідувальній або оперативно-розшуковій діяльності, досудовому розслідуванні -

карається штрафом від ста до трьохсот неоподатковуваних мінімумів доходів громадян або пробаційним наглядом на строк до трьох років, або обмеженням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

3. Дія, передбачена частиною другою цієї статті, якщо розголошені дані ганьблять людину, принижують її честь і гідність,–

карається пробаційним наглядом на строк від трьох до п'яти років або обмеженням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.»

Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341–14 (дата звернення: 11.06.2024).

2. Про контррозвідувальну діяльність: Закон України від 26.12.2002 № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374–15 (дата звернення: 11.06.2024).

ВИКОРИСТАННЯ КОНФІДЕНЦІЙНИХ МОЖЛИВОСТЕЙ ПІД ЧАС ОПЕРАТИВНО-РОЗШУКОВОЇ ПРОТИДІЇ КОЛАБОРАЦІЙНІЙ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

Олександр КРИВОШЕЙ
аспірант Харківського національного
університету внутрішніх справ

Агресивна війна, розв'язана російською федерацією проти України,– пекуча й текуча сучасність Українського народу, що поставила питання про базові засади соціальності, людяності, про колективну консолідацію, про життєздатність і дієвість мотиваційних двигунів європейської цивілізації. Супротив агресії – результуюча згущення волі, спрямованої на утримання соціально-часової, ціннісної, цивілізаційної дистанції з агресором засобами збереження української політичної нації. Задача – екстраординарна, з невизначеними вихідними даними. Їх визначення, адаптація, фіксація поточних (воєнних) змін, управління ними – одна з умови перемоги у війні. Кримінальна протиправність у вигляді колабораційної діяльності в структурі цих вихідних даних, значущих для перебігу і результатів війни факторів, посідає одне з визначальних місць, зважаючи на кримінальну природу самої агресії і проявів функціонування російського фашистського політичного режиму. Відтак ефективна протидія колабораційній діяльності та успішне ведення оборонної війни – категорії з одного ряду задач, хоча й з відмінним інструментарієм реалізації.

Чинне законодавство у ст. 1111 Кримінального кодексу України передбачає відповідальність за колабораційну діяльність [1]. Співпраця громадян України з країною-агресором рф може створювати серйозні загрози для національної безпеки та стабільності України. Зокрема, можна окреслити наступні ключові аспекти небезпеки такої співпраці:

1) підрив національної безпеки: співпраця з країною-агресором може стати інструментом для проведення розвідувально-підривної діяльності на користь рф (шпигунство, диверсійну діяльність, дестабілізацію ситуації в Україні та інші акції, що загрожують національній безпеці тощо);

2) поширення пропаганди та дезінформації: співпраця з рф може включати поширення пропаганди та дезінформації, що спрямовані на підрив довіри до української влади, суспільства та державної ідеї загалом;

3) порушення законності: громадяни, які співпрацюють з російською федерацією, можуть порушувати закони України, зокрема шляхом участі у терористичних акціях, контрабанді, розголошенні державних таємниць та іншої незаконної діяльності;

4) порушення суверенітету: співпраця з країною-агресором може сприяти порушенню територіальної цілісності та суверенітету України, зокрема шляхом підтримки терористичних організацій на окупованих територіях [2, с. 49–50].

Отже, співпраця громадян України з країною-агресором може несе серйозні наслідки для нашої і вимагає особливої уваги та заходів із боку українських правоохоронних структур для її запобігання та припинення.

Термін «колаборація», «колабораціонізм» походить від французького collaboration, що означає співпраця, співробітництво з ворогом. «Колабораціонізм» часто використовують для означення добровільної співпраці осіб, окремих груп чи прошарків населення окупованих територій з окупантами [3].

Слід відмітити, що колабораційні дії можуть відбуватися як на території, яка перебуває під контролем уряду України, так і на тимчасово окупованих територіях. Наприклад, на контрольованих урядом України територіях можуть мати місце дії, передбачені статтею 1111 Кримінального кодексу України: пропаганда у закладах освіти, фінансування незаконних збройних формувань, надання допомоги веденню воєнних дій проти Збройних Сил України та інші.

Колаборантів часто виявляють завдяки повідомленням свідків, які стали свідками їхніх дій. Такі свідки можуть надати правоохоронним органам інформацію про час, місце, обставини і осіб, які беруть участь у злочині. Крім того, правоохоронці можуть використовувати Інтернет для виявлення ознак колабораційної діяльності на контрольованих територіях. Наприклад, вони можуть перевіряти вебсторінки, соціальні мережі, блоги, форуми та месенджери на наявність громадських заяв потенційних колаборантів [4].

Враховуючи той факт, що зазначена норма є новою для вітчизняної правозастосовної практики, виникають проблемні питання щодо оперативно-розшукової протидії колабораційній діяльності за допомогою конфіденційних можливостей оперативних підрозділів.

Надаючи оцінку сучасному стану використання конфіденційної допомоги правоохоронним органам в Україні, зазначимо, що така діяльність, як і в минулому, негативно оцінюється переважною більшістю громади. Особи, які володіють важливою для правоохоронців інформацію або мають потенціал її систематичного отримування, як правило, не схильні до конфіденційної співпраці з оперативними підрозділами. Як свідчить практика, подолання такого ментального бар'єру можливе лише на індивідуальному рівні [5, с. 223].

Тому вирішення сучасних проблем організації конфіденційної роботи оперативних підрозділів має бути здійснене шляхом комплексного реформування інституту використання конфіденційного співробітництва в цілому, адже схожі проблеми властиві для багатьох оперативних підрозділів [6; 7; 8]. При цьому, має бути принципово вирішене завдання щодо створення дієвих інструментів контролю за реальними результатами роботи конфідентів та ефективністю використання їх допомоги під час оперативно-розшукової протидії колабораційній діяльності в умовах воєнного стану.

З метою підвищення ефективності використання конфіденційних можливостей під час оперативно-розшукової протидії колаборaційній діяльності в умовах воєнного стану нами вбачається перспективність здійснення навчання конфідентів можливостям кримінального профайлінгу. Ефективність використання оперативними джерелами технології, яка поєднує методи вербальної та невербальної психодіагностики з метою профілювання для доказової бази або запобігання протиправним діям за допомогою виявлення потенційно небезпечних осіб і ситуацій з використанням методів прикладної психології, стане дієвим засобом на етапі виявлення первинної оперативно-розшукової інформації щодо підготовки та вчинення колаборaційної діяльності, її перевірки і реалізації шляхом створення психологічного портрета колаборантів, визначення девіантної поведінки таких осіб тощо.

Окремо підкреслимо, що, залучаючи конфідентів під час документування колаборaційної діяльності, варто мати на увазі те, що така робота є лише засобом досягнення окремих (проміжних) результатів під час оперативно-розшукової протидії колаборaційній діяльності в умовах воєнного стану, який не може розглядатись як самостійний показник діяльності правоохоронних органів і оперативних підрозділів. Особливу увагу необхідно приділяти комплексному підходу до протидії кримінальній протиправності, покращенню якісного складу конфідентів, а не збільшенню її кількості.

Список використаних джерел:

1. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колаборaційну діяльність: Закон України від 03.03.2022 р. № 2108-IX. URL: https://zakon.rada.gov.ua/laws/show/2108–20/print (дата звернення 20.06.2024).

2. Кіреєва О.С. Використання кримінальними аналітиками інноваційних технологій для виявлення проявів колаборaційної діяльності.Електронний науковий періодичний журнал «Успіхи і досягнення у науці». 2024. Т. 1, № 3/3. С. 46–58. URL: https://doi.org/10.52058/3041–1254–2024–3(3)-46–58 (дата звернення: 20.06.2024).

3. Заєць О.М. Юридична характеристика дефініції колаборація. Актуальні питання кримінально-правової кваліфікації, документування та розслідування колаборaціонізму: матеріали Всеукраїнської науково-практичної конференції (Одеса, 21 липня 2022 року). Одеса, 2022. С. 45–46.

4. Коваленко А.В. Початковий етап розслідування колаборaційної діяльності, вчиненої на підконтрольних уряду України територіях. Протидія проявам тероризму та колаборaціонізму в умовах війни: стан та перспективи: матеріали Всеукраїнського круглого столу (м. Кропивницький, 24 листопада 2023 року). Донецький державний університет внутрішніх справ. Кропивницький, 2023. С. 34–37.

5. Драчова К.В. Індивідуальні оперативно-профілактичні заходи підрозділів карного розшуку щодо попередження грабежів та розбоїв, які вчиняють неповнолітні. Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали Міжнар. наук.– практ. конф. (Харків, 22 листопада 2013 р.). Харків: ХНУВС, 2013. С. 222–223.

6. Капустник В.В., Стащак М.В. Проведення оперативно-розшукових заходів, які потребують рішення прокурора: проблемні аспекти організаційного характеру. Науковий вісник Дніпропетровського ДУВС. 2019. Спецвипуск № 103. С. 32–42.

7. Давидюк В.М. Повноваження основних сил оперативно-розшукової діяльності в процесі протидії злочинності підрозділами НП України. Вісник Харківського національного університету внутрішніх справ. 2018. Спецвипуск № 1 (80). Ч. 2. С. 16–21.

8. Козаченко О.І. Сутність організації негласного співробітництва. Науковий вісник Національної академії внутрішніх справ. Ч. 2. 2015. № 2 (35). С. 134–146.

ПАРТНЕРСТВО СЛУЖБИ БЕЗПЕКИ УКРАЇНИ З НЕДЕРЖАВНИМ СЕКТОРОМ, ЯК ЗАСІБ ПІДВИЩЕННЯ ЇЇ СПРОМОЖНОСТЕЙ В СУЧАСНИХ УМОВАХ

Сергій КУДІНОВ
доктор юридичних наук, професор
головний науковий співробітник
Державної наукової установи
«Інститут інформації, безпеки і права
Національної академії правових наук України»
координатор проектів у сфері
національної безпеки (ГО»Safe Ukraine 2030»)

Військова, неспровокована агресія рф проти України з використанням заборонених засобів та способів війни, а фактично ведення її терористичними засобами – жорстокі вбивства мирних громадян (дітей та військових тощо), знищення цивільної інфраструктури (шкіл, лікарень, дитячих садків), використання голоду і холоду, як засобів впливу, переплетені з погрозами подальшого вчинення злочинів, у тому числі застосування ядерної зброї задля реалізації імперських амбіцій обумовили нову реальність виживання українців.

У протидії російсько-терористичному нападу на нашу країну, особлива роль відведена Службі безпеки України, як єдиному державному органу спеціального призначення, що здійснює протидію розвідувально-підривній діяльності проти України; боротьбу з тероризмом; контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, інформаційної безпеки держави, об'єктів критичної інфраструктури тощо [6].

У своїй злочинній діяльності країна агресор спирається на свій економічний потенціал, необмежені людські ресурси, використання досягнень науки і техніки, своїх прихильників у всьому світі.

Світ визнав необхідність збільшення витрат на безпеку, оборону, розвиток військового виробництва, об'єднання зусиль навколо створення умов безпечного існування тощо. При цьому, все це повинно відбуватися в умовах дефіциту ресурсів на реалізацію цих потреб й необхідністю їх пошуку. Не зважаючи на героїзм населення нашої країни, збройних сил, військових формувань сектору безпеки і оборони, потенціал країни агресора є набагато більшим.

Тому для нашої держави, її сектору безпеки і оборони актуальним залишається пошук додаткових ресурсів: матеріальних, фінансових, озброєння, інтелектуальних, людських для продовження боротьби за виживання нашої нації.

Одним із засобів їх пошуку є мобілізація ресурсів самого суспільства, шляхом розробки нових моделей, що забезпечують більш ефективне їх використання в сучасних умовах, створюють ефекти синергії тощо. Зокрема, мова йде про механізми партнерства, у першу чергу у сфері безпеки і оборони.

Так, у 1990-х роках в умовах скорочення бюджету ЦРУ на 25%, людські та матеріальні ресурси цього розвідувального органу були недостатні для швидкого й ефективного виконання його функцій, особливо напередодні атак 11 вересня 2001 року. Задля вирішення вказаної проблеми керівництво органу вдалося до масового використання «підрядників» [2; 4].

Дослідники питань партнерства державного і недержавного секторів зазначають, що фундаментальною причиною, яка веде до утворення партнерств, є усвідомлення факту, що приватний і публічний сектори мають унікальні характеристики, які забезпечують їм перевагу у наданні послуг населенню. Іншою засадничою передумовою формування і поширення практики

партнерств була і залишається зміна підходу до розуміння функцій урядів, зокрема усвідомлення необхідності передачі частини їх приватному сектору як більш мобільному й ефективному [7, С. 89].

У свою чергу, дослідники діяльності приватних розвідувальних компаній вказують на те, що вони є вагомим чинником сучасного безпекового середовища на глобальному рівні. З огляду на більшу еластичність у кадрових та фінансових питаннях приватні компанії мають суттєві переваги над державними органами в питаннях конкуренції за кращих спеціалістів; вони випереджають спеціальні служби у створенні та використанні новітніх технологій, які застосовують у розвідувальній діяльності [3, С. 17].

Слід зазначити, що хоч питання державно-приватного партнерства у цій сфері і не мають належного правового забезпечення, однак вже доволі розповсюджені у нашій країні – мова йде у-першу чергу про створення озброєння, спорядження, техніки. А от питання партнерства у сфері забезпечення державної безпеки пов'язують переважно з державними закупівлями, виконанням робіт, наданням благодійної допомоги, співробітництвом окремих громадян з органами державної безпеки тощо.

Ще у 2009 році було заявлено, що розвідувальні органи США витрачають більш як 70% бюджету на оплату роботи «підрядників», ЦРУ – близько 30% [2].

Колишній директор Агенції національної безпеки та Центрального розвідувального управління США М. Хайден, характеризуючи партнерство приватного і державного секторів у цій сфері, взагалі закликав не проводити межу між державними органами та представниками приватного бізнесу, значна частка яких готова ризикувати без грошової винагороди з метою допомоги у забезпеченні національної безпеки [2].

Оновлена Контртерористична стратегія ЄС на 2023–2027 роки також наголошує на тому, що у майбутньому важливу роль у протидії тероризму повинно-відігравати державно-приватне партнерство з організаціями приватного сектору. Воно може гарантувати, що новітні технологічні розробки не будуть доступні для терористів, а більш тісний зв'язок між цивільним суспільством і державними органами забезпечить узгодження зусиль у боротьбі з тероризмом, потребами і поглядами усіх верств населення, тим самим збільшуючи вірогідність їх більш широкого прийняття та використання [1].

На доцільності використання потенціалу державно-приватного партнерства було наголошено і в Стратегії національної контррозвідки США (2020–2022) [10]. Поряд із переліченим, до переваг використання приватних компаній в інтересах забезпечення державної безпеки слід віднести і можливість оперативного здобуття інформації, у тому числі за межами України (наявність зав'язків, спроможностей для здобування інформації), використання потенціалу приватних служб охорони та структур корпоративної безпеки, які зацікавлені у створенні безпечних умов для своїх підприємств, їх керівників та працівників. Більш того, вони готові інвестувати у заходи безпеки.

Розмірковуючи над питанням партнерства з приватними компаніями у сфері національної безпеки, колишній керівник Міністерства внутрішньої безпеки США М. Чертофф зазначає, що вирішальним чинником для наймання приватних компаній чи окремих осіб є їх унікальна кваліфікація або навички, на оволодіння якими може бути витрачено багато часу. Крім того, до «підрядників» звертаються, зазвичай, тоді, коли виникає тимчасова потреба у знаннях і вміннях у певній сфері. У цих випадках наймання спеціалістів заощаджує час і ресурси, оскільки «підрядники» не є постійними співробітниками, їх можна легко замінити за потреби. Це особливо актуально, коли законодавці ставлять перед розвідувальним співтовариством завдання, що потребують значних витрат, але при цьому скорочують бюджет [3, С. 10].

Доволі цікавим з точки зору врахування у забезпеченні державної безпеки, протидії тероризму є іноземний досвід створення спільнот у цій галузі. Так, орієнтирами у цьому напрямі можуть бути проекти «Griffin», «ECSA – CERBERUS», «ProtectUK» (Контртерористичний альянс) [8; 10].

ProtectUK створений у 2022 році та є результатом партнерства Національного управління по боротьбі з тероризмом (NaCTSO), Міністерства внутрішніх справ та Pool Re (провідної

британської компанії зі страхування ризиків тероризму) у Великій Британії, які втрьох відповідають за реалізацію цього проекту. У його основі лежить обмін інформацією та знаннями з метою використання досвіду та результатів досліджень для виявлення інноваційних підходів до інформування бізнесу і суспільства про терористичну загрозу, а також, кращих практик боротьби з нею. Крім того, це безкоштовний ресурс, що включає у себе велику кількість інформації, що допомагає підприємствам і організаціям розібратися з тим, що їм зробити для безпеки своїх організацій та їх клієнтів, у тому числі, навчання. Він знаходиться у віданні Національного управління по боротьбі з тероризмом, підрозділу поліції, що підтримує напрямок «захисту і підготовки» урядової стратегії боротьби з тероризмом [11].

Зазначений досвід набуває особливої актуальності в умовах підготовки СБУ правил антитерористичної безпеки в Україні [5].

Практика діяльності іноземних спеціальних служб та правоохоронних органів, приписи міжнародного законодавства дозволяють виокремити перспективні напрями посилення спроможностей Служби безпеки України шляхом партнерства з приватними підприємствами та їх структурами безпеки, серед яких:

- створення безпекових платформ (освітнього та інформаційно- комунікативного характеру);
- отримання оперативно-значущої інформації в інтересах забезпечення державної безпеки як в країні, так і за її межами, у тому числі її обробка;
- сприяння у використанні існуючих та розробка нових продуктів програмного забезпечення для пошуку, ідентифікації осіб, що створюють загрозу державній безпеці України, фіксацію їх злочинної діяльності тощо;
- здійснення аналітичних досліджень, узагальнення великого масиву даних в інтересах забезпечення державної безпеки, у тому числі розслідування воєнних злочинів;
- підготовка кадрів до роботи в сучасних умовах, у т.ч. з використанням новітніх технологій.

Слід зазначити, що не менш важливою умовою і навіть запорукою реалізації зазначених напрямів співпраці є прозорість, взаємна довіра та корисність такого партнерства, а також чітка правова регламентація прав й обов'язків сторін такого партнерства.

Список використаних джерел:

1. Контртерористична стратегія ЄС на 2023–2027 роки. URL: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a9ad67#_To c121816434 (дата звернення 18.06.2024).

2. Навіщо ЦРУ наймати підрядників? URL: https://www.golosameriki.com/a/cia-press-club-2009–08–20–53867882/660954.html (дата звернення 18.06.2024).

3. Паливода В.О. Приватні розвідувальні компанії: іноземний досвід залучення приватного сектору до виконання завдань розвідки. Аналітична доповідь. Київ: НІСД. 2022. 20 с. URL: https://niss.gov.ua/sites/default/files/2022–06/ad-privat-intell-comp1_gotove_04.pdf (дата звернення 18.06.2024).

4. Приватні розвідувальні компанії: іноземний досвід залучення приватного сектору до виконання завдань розвідки. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/pryvatni-rozviduvalni- kompaniyi-inozemnyy-dosvid-zaluchennya (дата звернення 18.06.2024).

5. Про затвердження Правил антитерористичної безпеки. Проект Постанови Кабінету міністрів України. URL: https://ssu.gov.ua ‘ 3-proekt- postanovi-kmu (дата звернення 18.06.2024).

6. Про Службу безпеки України: Закон України від 25.03.1992 № 2229- XII URL: https://zakon.rada.gov.ua/laws/show/2229–12#Text (дата звернення 18.06.2024).

7. Сімак С.В. Світовий досвід організації державно-приватного партнерства. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». Серія «Державне управління». 2014. Т. 235. Вип. 223. С. 88–93. URL: http://nbuv.gov.ua/UJRN/Npchdu_2014_235_223_18 (дата звернення 18.06.2024).

8. ECSA – Cerberus. Забезпечення безпеки та проведення розслідувань.URL: https://www.linkedin.com/showcase/ecsa-cerberus/about/ (дата звернення: 18.06.2024).

9. National Counterintelligence Strategy of the United States of America 2020–2022. Executive Summary. [Електроннийресурс].URL: https://www.dni.gov/files/NCSC/documents/features/20200205- National_CI_Strategy_ 2020_2022_Executive_Summary.pdf (дата звернення 18.06.2024).

10. Project Griffin (FromWikipedia, the free encyclopedia).URL: https://en.wikipedia.org/wiki/Project_Griffin (дата звернення: 18.06.2024).

11. Protect your business. Protect the public. Protectuk. URL: https://www.protectuk.police.uk/ (дата звернення 18.06.2024).

ЗАЛУЧЕННЯ ГРОМАДСЬКОСТІ У ПРОТИДІЇ КОНТРАБАНДІ ФАЛЬСИФІКОВАНИХ ЛІКАРСЬКИХ ЗАСОБІВ

Руслан ЛАВРОВ
співробітник СБУ

Контрабанда фальсифікованих лікарських засобів становить серйозну загрозу для життя та здоров'я людей, завдає колосальних збитків фармацевтичній галузі та підриває довіру до системи охорони здоров'я в цілому. Обсяги контрабанди фальсифікованих ліків невпинно зростають, а злочинці застосовують дедалі витонченіші методи для маскування своєї протиправної діяльності. [1]

Протидія цьому явищу вимагає комплексного підходу, який би поєднував зусилля правоохоронних органів, органів державної влади, фармацевтичних компаній та, що надзвичайно важливо, активну участь громадянського суспільства.

Передусім слід зазначити, що участь громадян у діяльності оперативних підрозділів правоохоронних органів можлива у різних формах: гласній, негласній та анонімній. Громадяни можуть надавати цінну інформацію про способи і маршрути контрабанди, місцезнаходження складів та осіб, причетних до незаконного обігу фальсифікованих ліків, канали їх розповсюдження, факти відмивання грошей тощо. Така первинна розвідувальна інформація є неоціненною для успішної протидії контрабанді.

Крім того, громадяни самі можуть долучатися до конфіденційного співробітництва з оперативними підрозділами, виконуючи спеціальні завдання, беручи участь у проведенні оперативно-розшукових заходів. Законодавство передбачає як гласні, так і негласні форми такої співпраці із забезпеченням конфіденційності та правового захисту громадян-помічників.

Системна робота із залучення допомоги населення дозволяє оперативним підрозділам підвищити свою професійність і компетентність у сфері протидії контрабанді фальсифікатів, оптимізувати використання ресурсів та зосередити зусилля на пріоритетних напрямках. Доступ до своєчасної достовірної інформації значно підвищує ефективність та оперативність дій правоохоронців у цій сфері.

Проте, на жаль, наразі існує низка проблем, що перешкоджають налагодженню ефективної співпраці громадян та оперативних підрозділів у протидії контрабанді фальсифікованих лікарських засобів. Першою і чи не найголовнішою з них є негативний соціальний статус осіб, які співпрацюють з правоохоронцями на конфіденційній основі. У суспільній свідомості досі побутує різко негативне сприйняття так званих «конфідентів» чи «інформаторів», що розглядаються як зрадники та безчесні люди.

Подолати ці стереотипи можна лише шляхом активної правової пропаганди в інститутах громадянського суспільства, широкого роз'яснення суспільної корисності та значущості участі

громадян у протидії злочинності. Необхідно донести до людей, що їхня допомога спрямована на захист життя, здоров'я, прав і свобод людини і громадянина, забезпечення безпеки суспільства від злочинних посягань.

Іншою вагомою перешкодою співпраці є відсутність належних соціальних та правових гарантій безпеки для осіб, що сприяють правоохоронним органам. Норми законодавства у цій сфері сформульовані доволі нечітко, «езоповою мовою», і фактично не розкривають усіх можливих заходів захисту та умов їх застосування.

Громадяни, які допомагають протидіяти злочинності, мають усвідомлювати, що вони перебувають під захистом держави, і бачити реальні практичні кроки із забезпечення їхньої безпеки у разі виникнення загроз. Відтак, принцип гласності й відкритості у цій сфері має бути невід'ємним складником формування довіри населення до правоохоронної системи.

Водночас, удосконалення самого законодавства у напрямку чіткого визначення соціальних гарантій, порядку застосування заходів захисту, можливості звільнення від кримінальної відповідальності за певних умов тощо, матиме неабияке значення для активізації співпраці громадян з оперативними підрозділами.

Нарешті, вагомим стимулом для сприяння громадян може стати впровадження системи винагород і заохочень для осіб, інформація чи дії яких допомогли попередити або розкрити контрабанду фальсифікованих лікарських засобів. Гідна фінансова чи інша матеріальна винагорода в поєднанні з гарантіями безпеки та соціального захисту може стати потужним каталізатором для формування мереж громадських помічників в усіх регіонах.

Підсумовуючи, слід наголосити, що сприяння громадян є ключовим елементом у протидії контрабанді фальсифікованих ліків і має неоціненне значення для підвищення ефективності роботи правоохоронців у цій сфері. Проте наразі через ряд об'єктивних причин цей потенціал використовується не повною мірою. Тож системне вирішення порушених проблем шляхом розробки комплексної програми співпраці з громадянами, удосконалення законодавства, широкої інформаційної кампанії та посилення гарантій захисту і винагород для помічників правоохоронців, сприятиме нарощуванню зусиль у протидії контрабанді фальсифікованих лікарських засобів та досягненню відчутних успіхів у цьому напрямку.

Лише за умови консолідації держави, правоохоронної системи та інститутів громадянського суспільства можливо успішно протистояти загрозам, які несе контрабанда фальсифікованих ліків для здоров'я нації та національної безпеки.

На наш погляд, враховуючи сучасний стан протидії контрабанді фальсифікованих лікарських засобів необхідно:

1. Розробити комплексну цільову програму налагодження ефективної співпраці органів, що протидіють контрабанді фальсифікованих лікарських засобів, та громадськості. Ця програма має охопити законодавчі, організаційні, інформаційно-пропагандистські та матеріально-технічні аспекти взаємодії. До її розробки доцільно залучити представників правоохоронних і контролюючих органів, фармацевтичної галузі, експертного середовища та громадянського суспільства.

2. В рамках зазначеної Програми ініціювати внесення змін до законодавства у частині чіткого визначення соціальних гарантій для громадян, що сприяють правоохоронцям, порядку застосування заходів їх захисту, можливостей звільнення від кримінальної відповідальності за певних умов тощо. Доцільно також передбачити механізми роботи з анонімними джерелами інформації.

3. Паралельно із законодавчими змінами започаткувати системну інформаційну кампанію в медіа, соціальних мережах та інших публічних майданчиках з метою роз'яснення суспільної корисності та значущості сприяння громадян правоохоронним органам у боротьбі зі злочинністю. Наголошувати на принципах гласності, відкритості та прозорості у цій сфері.

4. Посилити гарантії безпеки та соціального захисту для громадян, що сприяють протидії контрабанді фальсифікованих лікарських засобів, зокрема через запровадження системи винагород та заохочень за результативну допомогу оперативним підрозділам. Механізми нарахування та виплати винагород повинні бути прописані максимально прозоро.

5. Активізувати налагодження довірчих контактів між працівниками оперативних підрозділів та громадськими активістами, лідерами думок у місцевих громадах з метою формування мереж громадських помічників у всіх регіонах країни.

Комплексна реалізація наведених рекомендацій дозволить підвищити ефективність протидії контрабанді фальсифікованих лікарських засобів шляхом максимального використання потенціалу допомоги з боку громадянського суспільства.

Список використаних джерел:

1.Фальсифіковані лікарські засоби і відповідальність за фальсифікацію. URL: https://www.dls.gov.ua/for_subject/%D 1 %84 %D 0 %B 0 %D 0 %BB%D 1 %8C%D 1 % 81%D0%B8%D1%84%D1%96%D0%BA%D0%BE%D0%B2%D0%B0%D0%BD%D1%96- %D0%BB%D1% 96%D0%BA %D0%B0%D1%80%D1% 81%D1%8C%D0%BA% D1%96- %D0%B7%D0%B 0%D1%81%D0%B E%D0%B 1%D0%B8-%D1%96-%D0%B2%D1%96/ (дата звернення: 20.06.2024).

ЩОДО ПРОТИДІЇ ОРГАНІЗОВАНИМ ЗЛОЧИННИМ УГРУПОВАННЯМ, ЯКІ ЗАГРОЖУЮТЬ ДЕРЖАВНІЙ БЕЗПЕЦІ УКРАЇНИ

Юрій ЛУЦЕНКО
доктор юридичних наук, професор
співробітник НМНДЦ при РНБО

Стрімкий розвиток суспільних правовідносин, демократизація державних інституцій неможлива без наступальної боротьби зі злочинністю у різних її проявах. Держава в особі компетентних органів визначає правила поведінки, що спрямовані на гарантування безпеки кожній особі, а також встановлення стану захищеності суспільства та держави від різного роду протиправних посягань на охоронювані інтереси. Порушення цих приписів може призвести до завдання непоправної шкоди ефективній діяльності держави у різних її сферах [1, с. 389]. У зв'язку із зростанням суспільної небезпеки перед державою постає питання щодо забезпечення ефективної охорони як окремого громадянина, так і всього суспільства в цілому [2, с. 5].

Сьогодні важливу роль у боротьбі з організованою злочинністю відіграють Національні програми (Стратегії), прийняті урядами багатьох держав світу. Першочергова увага в цих програмах приділена створенню механізмів і системи ефективного контролю, у тому числі і за роботою недержавних організацій, і широкого спектру незалежних засобів масової інформації. З метою проведення ефективної політики у сфері боротьби з організованою злочинністю у більшості держав створені і діють громадські організації, парламентські комісії та державні установи [3].

Так, наприклад, в Україні Розпорядженням КМ України від 16.09.2020 № 1126-р схвалено Стратегію боротьби з організованою злочинністю (далі – Стратегія). Дана Стратегія визначає напрями розвитку системи боротьби з організованою злочинністю та механізми реалізації державної політики у відповідній сфері в сучасних умовах.

Водночас, МВС України, СБУ, ГУР МО України, Мініюст, РНБО України, а також іншими зацікавленими державними органами розроблено розпорядження КМ України «Про затвердження плану заходів з реалізації Стратегії боротьби з організованою злочинністю» [4] (далі – План заходів з реалізації Стратегії).

Даним Планом заходів з реалізації Стратегії визначено наступний механізм звітування про виконання: Міністерство внутрішніх справ щороку подає КМ України звіт про виконання Плану заходів з реалізації Стратегії.

Водночас, Стратегією боротьби з організованою злочинністю передбачено постійне проведення оцінки стану реалізації Плану заходів з реалізації Стратегії на підставі виконання Плану заходів з її реалізації. Така оцінка стану реалізації зазначеного Плану подається Національним координатором (має бути утворений як міжвідомча комісія – координаційний орган) КМ України, Президентові України та ВР України.

Тимчасово, до моменту утворення Національного координатора, Планом заходів з реалізації Стратегії передбачено визначення державного органу, відповідального за підготовку щорічної оцінки стану реалізації державної політики у сфері боротьби з організованою злочинністю та спеціальних звітів про стан організованої злочинності в Україні, основні напрями та результати боротьби з організованою злочинністю. Отже, запропоновані у Плані заходи з реалізації Стратегії суб'єкти, адресати, форма і терміни подання узагальнених матеріалів про стан реалізації Стратегії боротьби з організованою злочинністю не відповідають тим, що визначені у схваленій Урядом Стратегії.

Також необхідно зазначити, що загальним недоліком Плану заходів з реалізації Стратегії є наскрізне формулювання – «розроблення та вжиття заходів». Видається, що під відповідні визначені Планом заходів з реалізації Стратегії заходи виникне необхідність на міжвідомчому рівні розробляти додаткові заходи, а отже і плани таких заходів. Відтак, сам План заходів з реалізації Стратегії втрачатиме роль організуючого документа. Вважаємо, що застосування слова «захід» у контексті виконання «завдання» не може зводитися до відсилки до чогось наразі неіснуючого та неконкретного.

План заходів містить ініціативу з розроблення законопроекту про внесення змін до Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» щодо визначення Нацполу головним органом боротьби з організованою злочинністю, що виходить за межі відповідних приписів Стратегії. Схвалена стратегічна позиція про систему інституційного забезпечення боротьби з організованою злочинністю передбачає функціонування державних органів, основною функцією яких є боротьба з організованою злочинністю (спеціально визначений підрозділ у структурі Нацполу та оперативні підрозділи СБУ), без визначення головного з цих органів. Водночас, вважаємо, що узгоджуватиметься зі Стратегією розроблення змін до вказаного Закону щодо віднесення визначеного структурного підрозділу Національної поліції до переліку державних органів, спеціально створених для боротьби з організованою злочинністю (ст. 5 Закону), а також надання йому відповідних повноважень, у т.ч. пов'язаних із використанням штатних і нештатних негласних співробітників (ст. 13 Закону). Необхідним також є одночасне внесення відповідних змін і до Закону України «Про Національну поліцію», згідно з яким наразі у загальній системі поліції немає спеціальних підрозділів, що здійснюють безпосередньо боротьбу з організованою злочинністю.

Необхідно також відмітити, що План заходів з реалізації Стратегії передбачає проведення аналізу нормативно-правових актів у сфері боротьби з організованою злочинністю, виявлення положень, що потребують вдосконалення, підготовку пропозицій. Водночас, до числа співвиконавців цього заходу не залучено СБУ, що, у подальшому, може призвести до залишення без належної уваги законодавчих ініціатив, напрацьованих спецпідрозділами по боротьбі з корупцією та організованою злочинністю СБУ у ході багаторічної ефективної правозастосовної практики у сфері боротьби з організованою злочинністю.

Аналогічне зауваження стосується і вивчення питання про розмежування та конкретизацію повноважень органів, які здійснюють боротьбу з організованою злочинністю, з метою усунення дублювання їх функцій, а також розроблення та затвердження проекту міжвідомчого наказу щодо організації взаємодії у сфері боротьби з організованою злочинністю. Відсутність СБУ серед співвиконавців відповідних заходів, на нашу думку, є неприпустимою, оскільки вирішення вказаних питань впливатиме на обсяг повноважень уповноважених оперативних підрозділів СБУ (визначених за результатами реформування) та їх участь у міжвідомчій взаємодії [5, с. 141].

Отже, є необхідність у включенні СБУ до числа співвиконавців Плану заходів з реалізації Стратегії, які належать до компетенції або стосуються обсягу повноважень СБУ.

Не вирішеним залишається питання щодо розроблення проекту постанови КМ України про утворення координаційного органу (Національного координатора) – Міжвідомчої комісії боротьби з організованою злочинністю та затвердження положення, посадового складу, керівника та заступників керівника вказаної комісії (запровадження механізмів координації та взаємодії у сфері боротьби з організованою злочинністю), на нашу думку, не може опрацьовуватися одноособово МВС України. Оскільки майбутня діяльність цієї Міжвідомчої комісії повинна базуватися з додержанням принципу колегіальності, до визначення основоположних засад її функціонування та формування персонального складу очевидно мають бути залучені й інші суб'єкти боротьби з організованою злочинністю. До її керівного складу доцільно включити на рівних правах (як співголови комісії) представників державних органів, основною функцією яких є боротьба з організованою злочинністю, тобто Нацполу та СБУ (або їх уповноважених підрозділів).

Також необхідно зазначити, що у межах чисельності наявних органів державної влади, що проводять свою діяльність у сфері боротьби з організованою злочинністю, Національний координатор повинен бути рівнонаближеним до всіх суб'єктів боротьби з організованою злочинністю, таким органом наразі є РНБО України до якого можуть відряджатися представники від усіх уповноважених суб'єктів боротьби з організованою злочинністю.

Крім того, при вирішенні питання про утворення координаційного органу (Національного координатора) варто враховувати, що у п. 2 ст. 4 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» передбачено, що підзаконні акти, які регулюють відносини у сфері боротьби з організованою злочинністю, не можуть встановлювати повноваження державних органів чи обов'язки фізичних та юридичних осіб, які не випливають із законів України. Відтак, замість проекту акта КМ України про утворення Національного координатора слід підготувати та внести на розгляд до ВР України відповідний законопроект.

Поза увагою упорядників Плану заходів з реалізації Стратегії залишилось передбачене Стратегією питання про виявлення, ліквідацію кримінальних мереж, відстеження грошових потоків і повернення активів, одержаних від корупційних та інших кримінальних правопорушень. При цьому, однією з ідентифікованих загроз організованої злочинності в Україні, зазначених у Стратегії, є установлення корумпованих відносин між посадовими особами органів державної влади, органів місцевого самоврядування та криміналітетом. Тож видається доцільним передбачити у Плані заходи з реалізації Стратегії, які будуть спрямовані на руйнування злочинної співпраці між окремими представниками державної влади та злочинними угрупованнями, насамперед транснаціональними, усунення із займаних посад та притягнення до передбаченої законом відповідальності очільників державних органів, що мають корупційні зв'язки з кримінальними бізнес-структурами, повернення законним власникам активів, що стали предметом корупційних та інших кримінальних правопорушень [5, с. 141–142].

При нагоді необхідно звернути увагу, що протидія організованій злочинності потребує комплексного підходу з врахуванням національного досвіду та принципово нових підходів, які мають ґрунтуватися на потребах забезпечення національної безпеки держави у цілому за безпосередньої участі органів СБУ.

Аналіз змісту чинної Стратегії національної безпеки України [6] дозволяє віднести до актуальних кримінальних загроз національній безпеці України такі:

– агресивні дії Росії, що здійснюються для виснаження української економіки й підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, а саме: розвідувально-підривна і диверсійна діяльність, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі й ненависті, сепаратизму й тероризму, створення і всебічна підтримка, зокрема військова, маріонеткових квазідержавних утворень на тимчасово окупованій території частини Донецької та Луганської областей (п. 3.1);
– неефективність системи забезпечення національної безпеки і оборони України: діяльність незаконних збройних формувань, зростання злочинності, незаконне використання вогнепальної зброї (п. 3.2);

– корупція та неефективна система державного управління: поширення корупції, її укорінення в усіх сферах державного управління (п. 3.3).

Отже, можна дійти висновку, що злочинність (не лише організована чи транснаціональна) становить суттєву внутрішню загрозу національній безпеці України. При цьому в безпековому контексті доцільно розглядати реальні та потенційні прояви злочинності, які створюють загрози життєво важливим інтересам України (а також її фонові явища) як кримінальні загрози національній безпеці в цілому або її окремим складовим.

Принагідно, необхідно зазначити, що потреба участі уповноважених підрозділів національної спецслужби у сфері протидії транснаціональній організованій злочинності зумовлена тим, що діяльність інших правоохоронних органів України передбачає застосування лише оперативно-розшукових та кримінальних процесуальних заходів, тоді як сьогодні існує необхідність у застосуванні широкого спектру можливостей контррозвідувальної діяльності, котра є прерогативою тільки СБУ.

Варто також зазначити, що на доцільність участі спецслужб у виконанні завдань щодо протидії організованій злочинності та корупції вказує й міжнародний досвід (так, подібні завдання виконують практично всі спеціальні служби країн пострадянського простору, Німеччини, Ізраїлю, Естонії, Латвії, Іспанії, Польщі, США. Зокрема, ФБР США, одним із головних пріоритетів якого є протидія корупції у публічному секторі, вважається зразком комплексного підходу до забезпечення національної безпеки).

Виходячи із зазначеного, вбачається за доцільне:

1. Включити СБУ до числа співвиконавців Плану заходів з реалізації Стратегії, відносно тих питань, які належать до компетенції або стосуються обсягу повноважень національної спецслужби.

2. Доповнити ч. 1 ст. 19 Закону України «Про національну безпеку України» пп. 5 такого змісту: «попередження, виявлення, припинення діяльності злочинних організацій у сфері управління та економіки, громадської безпеки та розкриття злочинів проти миру і безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України».

Список використаних джерел:

1. Луценко Ю.В., Тарасюк А.В. Актуальні проблеми удосконалення окремих положень кримінального та кримінального процесуального законодавства України. Юридичний науковий електронний журнал. 2023. № 1. С. 388–391.

2. Луценко Ю.В. Звільнення від кримінальної відповідальності за злочини проти основ національної безпеки України: монографія. Харків: Право. 2015. 200 с.

3. Інформація до роздумів: міжнародний досвід боротьби з корупцією. URL: http://stepup.press/antikorculture/ item/404-informatsiya-k-razmyshleniyumezhdunarodnyj-opyt-borby-s-korruptsiej (дата звернення: 15.06.2024).

4. Про затвердження плану заходів з реалізації Стратегії боротьби з організованою злочинністю. Розпоряд. Кабінету Міністрів України від 27.09.2022 № 850-р. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planuzakhodiv-z-realizatsii-stratehii-borotby-z-orhanizovanoiu-zlochynnistiu-850–270922 (дата звернення: 15.06.2024).

5. Луценко Ю.В. Проблеми організації протидії організованим злочинним угрупованням, які загрожують державній безпеці України. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2024. Том 35 (74) № 1. С. 139–146.

6. Стратегія національної безпеки України. Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 15.06.2024).

ОКРЕМІ ЗАСАДИ ВЗАЄМОДІЇ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ З ІНШИМИ СУБ'ЄКТАМИ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ, ЩО ВЧИНЯЄТЬСЯ З ВИКОРИСТАННЯМ МЕРЕЖІ ІНТЕРНЕТ

Олексій ЛЯШЕНКО
аспірант Національної
академії внутрішніх справ

На сьогодні світові тенденції зміни структури злочинності переконливо свідчать про зростання ролі інформаційно-телекомунікаційних технологій, які спричиняють появу принципово нових видів кримінальних правопорушень та активне вдосконалення «традиційної» злочинної діяльності. Комп'ютерні мережі, комунікаційні системи стали інструментом злочинців, унаслідок чого криміналізувалася сфера використання інформаційно-телекомунікаційних технологій [1]. У злочинців у мережі Інтернет велика ступінь анонімності, а інформація в комп'ютерних системах має короткостроковий характер зберігання. Враховуючи особливості злочинів у сфері інформаційно-комунікаційних технологій, важливе значення для результативності їх розкриття має взаємодія оперативних підрозділів поліції на всіх рівнях, в тому числі із представниками правоохоронних органів інших країн [2].

Важливо зазначити, що характерними особливостями злочинів, пов'язаних з торгівлею людьми, є: організованість і транскордонність (широкі міжрегіональні та міжнароднізв'язки); висока латентність, спричинена небажанням потерпілих повідомляти правоохоронні органи про вчинення відносно них цього злочину; високий рівень технічного забезпечення правопорушників [3, с. 85]. Таким чином, у цьому контексті особливого значення набуває діяльність підрозділів протидії кіберзлочинам щодо застосування спеціальних знань у процесі виявлення та фіксації слідів торгівлі людьми в Інтернет-мережах [4, с. 46].

Департамент кіберполіції, який забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, сприяє іншим підрозділам у попередженні, виявленні та припиненні кримінальних правопорушень. Одним із головних завдань кіберполіції є створення безпечного кіберсередовища для активних користувачів Інтернету [5].

Крім того, кіберполіцейські звертають увагу інтернет-користувачів на той факт, що інколи зловмисники викуповують доменні імена сайтів, які раніше добросовісно надавали послуги покупцям, і намагаються видати новий сайт за ресурс, який надає такі самі послуги, а інколи навіть може мати такий самий вигляд, як і старий ресурс [6].

Окремо потрібно звернути увагу на взаємодію оперативних працівників міграційної поліції з Департаментом стратегічних розслідувань Національної поліції [7]. Даний підрозділ утворений з метою підвищення ефективності діяльності органів і підрозділів Національної поліції під час виконання завдань із забезпечення прав і свобод людини та протидії злочинності. Його основними функціями є виявлення і документування протиправної діяльності суспільно небезпечних кримінальних угруповань в регіонах, а також кримінальних «авторитетів» і так званих «злодіїв у законі», організованими групами і злочинними організаціями [8, с. 136].

Отже, з огляду на викладене та ураховуючи узагальнені результати опитування респондентів встановлено, що з метою ефективної протидії торгівлі людьми з використанням мережі Інтернет, працівники міграційної поліції найчастіше здійснюють взаємодію на відомчому та міжвідомчому рівнях з такими суб'єктами: на відомчому рівні з підрозділами: кіберполіції – 97%; стратегічних розслідувань – 91%; карним розшуком – 91%; на міжвідомчому відомчому рівні з підрозділами: Служби безпеки України – 94%; Бюро економічної безпеки України – 91%; Державної прикордонної служби – 87%; Державної міграційної служби – 84%.

Список використаних джерел:

1. Тарасенко О.С. Теорія та практика протидії кримінальним правопорушенням, пов'язаним з обігом протиправного контенту в мережі Інтернет: монографія. Одеса: Видавничий дім «Гельветика», 2021. 426 с.
2. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / О.Є. Користін, В.М. Бутузов, В.В. Василевич та ін. Київ: Скіф, 2012. 728 с.
3. Бєляков Р.Г. Взаємодія управління боротьби з кіберзлочинністю МВС України з іншими правоохоронними органами: питання сьогодення. Право і безпека. 2014. № 4 (55). С. 85–88.
4. Павленко С.О. Тактика протидії торгівлі людьми органами Національної поліції України: вітчизняний та зарубіжний досвід. *Міжнародний науковий журнал «Інтернаука».* Серія: «Юридичні науки». 2018. № 5(10). С. 41–55. URL: https://doi.org/10.25313/2520–2308–2018–5–4020 . (дата звернення: 18.06.2024)
5. Звіт про результати роботи Департаменту кіберполіції у 2022 році. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u – roczi-969/ . (дата звернення: 18.06.2024)
6. Шахрайські інтернет-магазини: як зрозуміти, що вас обдурюють. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-moshennicheskie-internet-magaziny-kak-ponyat-chto-vas-obmanyvayut . (дата звернення: 18.06.2024)
7. Про утворення територіального органу Національної поліції постанова кабінету Міністрів України № 867 від 09 жовтня 2019 р. URL: https://zakon.rada.gov.ua/laws/show/867–2019-%D0%BF#Text . (дата звернення: 18.06.2024)
8. Севрук В.Г. Департамент стратегічних розслідувань національної поліції України як суб'єкт протидії злочинам, що вчиняють організовані групи та злочинні організації, сформовані на етнічному підґрунті. Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід: матеріали Міжнародного науково-практичного круглого столу, м. Київ, 19 лютого 2020 р. Київ: Національна академія внутрішніх справ, 2020. С. 134–136.

СТВОРЕННЯ «СІРИХ ЗОН» ЯК ІНСТРУМЕНТ ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ ТА МЕТОД ДЕСТАБІЛІЗАЦІЇ ОБСТАНОВКИ В КРАЇНІ

Василь МАЛЮК
кандидат юридичних наук

Гібридна війна починається не пострілами гармат та уведенням збройних сил на територію іншої країни. Цим діям передує підготовка у вигляді формування «п'ятої колони», створення внутрішніх загроз, у тому числі і з використанням злочинних об'єднань, які вже діють на території іншої країни. Найбільш ефективним у цьому контексті для спецслужб рф є транснаціональні організовані злочинні об'єднання, які «представлені» в Україні злочинними спільнотами «ворів у законі», оскільки вони вже діють практично як агентурні групи на чужій території, використовують контрагентурні методи, підтримують шифрований зв'язок та інші способи прихованої діяльності, протиставляючи себе державним інституціям. В Україні завдання інфільтрації спецслужб рф у такі групи було полегшеним, оскільки злочинні спільноти «ворів у законі» діють у всіх країнах колишнього СРСР, не визнаючи кордонів і фактично являючи собою систему підпорядкування з власними правилами та механізмами управління, яка діє і «розповсюджується» на територію декількох країн. Оскільки злочинні спільноти «ворів у законі» – це практично «продукт» рф (Російської імперії, СРСР), то відповідно і умовний

«центр керування» знаходиться там же. Тобто, узявши під контроль кримінальних лідерів у росії, спецслужби рф водночас отримують можливість використовувати їх злочинний вплив і в Україні. У результаті реалізації зазначених планів спостерігається тенденція інтегрування представників і лідерів злочинних спільнот у владно-управлінські структури, призначення на посади в органах центрального і місцевого самоврядування осіб, які надалі приймають управлінські рішення при розподілі бюджетних засобів, матеріальних ресурсів; інвестиційних програм і приватизації об'єктів державної і комунальної власності. Ще у 1998 році в 10 регіонах України, СБУ зафіксовано 32 таких факти (зокрема, в АРК вони намагалися активно впливати на процеси приватизації промислових об'єктів Червоноперекопського промвузла, Феодосійського, Керченського, Ялтинського морських портів, Феодосійської нафтоперевалочної бази, санаторно-курортного комплексу [1, с. 12].

Соціально-політичні зміни безпосередньо вплинули на міжнародний характер організованої злочинності. Транснаціональні злочинні спільноти намагалися розширити сфери впливу за рахунок проникнення до нашої країни, використовуючи набутий кримінальний досвід, апробують нові способи вчинення злочинів і захисту своєї злочинної діяльності [2, с. 10]. Наприкінці 90-х років стають наявними ознаки створення кількох політико-економічних груп кримінально-олігархічного типу, які починають відігравати в Україні роль найважливіших після держави елементів політичної системи. Спостерігається тенденція посилення контролю над найприбутковішими галузями економіки держави (металургійна, спиртова, хімічна, паливно-енергетичний комплекс), активізації їх у сферах фінансово-кредитної, насамперед банківської діяльності, приватизаційних та зовнішньоекономічних процесах (чітко простежується тенденція підпорядкування загальнокримінальної організованої злочинності та окремих груп, що входять до неї, більш могутнім кримінально-олігархічним кланам та їх зрощення).

Що стосується інтеграції кримінальних організацій пострадянських країн, зокрема України, з міжнародними синдикатами, то науковці визначають наступні основні напрямки: співробітництво при посередництві сицилійської мафії з колумбійськими картелями з метою створення у Центрально-Східній Європі та СНД ринку кокаїну; спільна участь вітчизняних, колумбійських та сицилійських мафіозі в обмінних операціях типу наркотики – зброя – ядерні матеріали для арабських країн; по-третє, співробітництво пострадянської організованої злочинності з азійськими тріадами у сфері налагодження каналів нелегальної міграції до країн Західної Європи; кооперація вітчизняних угруповань та сицилійської мафії на терені легалізації фальшивих і «брудних» доларів на території держав Східної Європи та СНД, участь у приватизаційних процесах в Україні та у регіоні взагалі; співробітництво вітчизняних кримінальних організацій та європейських угруповань у сфері постачання живого товару на ринки сексуальних послуг до країн Західної і Південної Європи [3, с. 20]. Серед зазначених зв'язків «приховуються» інтереси спецслужб рф (представлені злочинними спільнотами «ворів у законі»).

Якщо на попередньому етапі метою проникнення злочинних об'єднань в органи державної влади та їх корупціонування була нейтралізація правоохоронних заходів то поступово метою зазначених кланів (а відповідно і інфільтрованих в їх середовище представників злочинних об'єднань) стає економічна експансія. Хоча злочинні об'єднання переслідують економічні, а не політичні цілі, для їх досягнення використовуються і відверто терористичні методи – у 1997 році в аеропорту м. Донецька вбито народного депутата Є. Щербаня, у 1998 році в м. Києві у під'їзді свого будинку вбито народного депутата України В. Гетьмана.

Практично найбільш помітним був створений злочинний тандем взаємовигідних альянсів російських і українських злочинних угрупувань на територіях Донецької та Луганської областей. Результатом цієї спецоперації російських спецслужб був прихід до влади «донецьких» на чолі з Януковичем, який (разом з командою своїх поплічників, що зайняли переважну більшість ключових державних посад) відверто лобіював інтереси росії в Україні – аж до відмови від європейського курсу розвитку держави. Тобто, ще до початку прихованої агресії керівництво рф використовувало транснаціональну організовану злочинність в Україні з метою вирішення своїх інтересів, у тому числі й геополітичних. Після провалу цього плану Кремль

обирає інший шлях. Спостерігається тенденція втручання кримінальних структур у сфери зовнішньої торгівлі, розподілу ресурсів, відбувається криміналізація товарних ринків, що призводить до криміналізації усієї системи економічних відносин, в яких усе більшого значення набувають так звані «сірі зони» [4, с. 126], які на території України фактично створила рф, організувавши та підтримавши збройними силами сепаратистів на Сході України. «Сірі зони» за загальним поняттям є географічною територією, яка не контролюється легальною владою, і саме на цих територіях виникають злочинні організації, які розвивають «нелегальну економіку», що заснована на злочинних видах «бізнесу» (випуск контрафактної продукції, виробництво наркотиків тощо). Науковці до таких «сірих зон» відносять у Латинській Америці – окремі регіони Перу, Болівії, Колумбії (у цих регіонах владу зосереджено в руках наркокартелей), в Азії – Афганістан, в Африці – Ангола, Сьєрра-Леоне, Ліберія, у Росії – Чечня [4, с. 126].

Тобто окремі регіони Донбасу не стали «сірою зоною» самостійно, а цілеспрямовано були перетворені у злочинний анклав на території України спецслужбами рф, внаслідок насадження сепаратистської політики, створення штучних «псевдо» владних структур «ЛНР», «ДНР» з фактично злочинних угруповань, які культивувалися спецслужбами рф тривалий час і були використані для захоплення влади на окремих територіях Донецької та Луганської областей (на території суверенної держави – України) збройним шляхом. Весь час існування зазначених «псевдо» республік росія намагалася легітимізувати їх владу у різні способи – від офіційного визнання країнами-сателітами (або таким ж «псевдо» республіками – «сірими зонами», які були створені у такий же спосіб на території Молдови – Придністровська Молдавська Республіка; Грузії – Республіка Південна Осетія) до намагань увести як третю сторону до переговорної контактної групи у Мінську. А практично, у цих псевдоутвореннях керують злочинні угруповання, які «легітимізувалися» за допомогою та під керівництвом спецслужб росії, але за цією «ширмою» вчиняють весь спектр злочинів, що притаманні транснаціональним злочинним організованим об'єднанням.

Список використаних джерел:

1. Батиргареєва В.С. Рецидивна злочинність в Україні: соціально-правові та кримінологічні проблеми: монографія. Х.: Право, 2009. 576 с

2. Мінка П.Я., Чаплинський К.О. Тактика розслідування злочинів, вчинених організованими групами та злочинними організаціями: навчальний посібник. Дніпропетровськ: Дніпропетровський гуманітарний інститут, 2007. 221 с.

3. Дорошенко А. Терор і тероризм. Політика і час. 1997. № 8. С. 14–21.

4. Жаровська Г.П. Теорія та практика протидії транснаціональній організованій злочинності в Україні: дис. … докт. юрид. наук: 12.00.08. К. 2019. 595 с.

ДЕЯКІ ПИТАННЯ НОРМАТИВНО-ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ВИКОНАННЯ СПЕЦІАЛЬНОГО ЗАВДАННЯ З РОЗКРИТТЯ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ОРГАНІЗОВАНОЇ ГРУПИ ЧИ ЗЛОЧИННОЇ ОРГАНІЗАЦІЇ

Віталій МАЦАК
кандидат юридичних наук

Одним із важливих результатів реформування системи кримінальної юстиції в Україні є вдосконалення нормативно-правового регулювання досудового розслідування кримінальних правопорушень, озброєння правоохоронних органів сучасними інструментами його здійснен-

ня й намагання вдосконалити організаційні та правові засади кримінального переслідування відповідно до передової іноземної практики. Реалізація зазначеного відбувалася шляхом втілення прогресивного світового досвіду організації протидії протиправній діяльності у кримінальному процесуальному законодавстві України, що, зокрема, знайшло свій прояв у детальній правовій регламентації провадження як гласних, так і негласних слідчих (розшукових) дій. Водночас вказана реформа впливає не тільки на зміст чинного Кримінального процесуального кодексу України (далі – КПК України), а й загалом докорінно змінює засади розслідування злочинів. Одним із важливих інструментів такої діяльності є саме виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації, що входить до системи НСРД, загальні засади організації якої регламентуються ст. 272 КПК України. Водночас можливість якісного й успішного його проведення нерозривно пов'язана з досконалим правовим регулюванням, що потребує відповідного наукового супроводження [1, с. 183].

Аналіз нормативного забезпечення застосування оперативно-розшукових заходів та негласних слідчих (розшукових) дій показав, що окремі питання виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації на сьогодні регулюється низкою законів та відомчих нормативних актів.

Так, у Кримінальному процесуальному кодексі України серед негласних слідчих розшукових дій виділено «Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації». Зокрема, статтею 272 визначено, що під час досудового розслідування тяжких або особливо тяжких злочинів можуть бути отримані відомості, речі і документи, які мають значення для досудового розслідування, особою, яка відповідно до закону виконує спеціальне завдання, беручи участь в організованій групі чи злочинній організації, або є учасником зазначеної групи чи організації, який на конфіденційній основі співпрацює з органами досудового розслідування. Також встановлено, що виконання зазначеними особами такого спеціального завдання, як негласна слідча (розшукова) дія, здійснюється на підставі постанови слідчого, погодженої з керівником органу досудового розслідування, або постанови прокурора із збереженням у таємниці достовірних відомостей про особу. Крім того передбачено, що виконання спеціального завдання не може перевищувати шість місяців, а в разі необхідності строк його виконання продовжується слідчим за погодженням з керівником органу досудового розслідування або прокурором на строк, який не перевищує строку досудового розслідування [2].

Особливості кримінальної відповідальності осіб, які відповідно до закону виконувала спеціальне завдання, беручи участь в організованій групі чи злочинній організації з метою попередження чи розкриття їх кримінально протиправної діяльності визначено у статті 43 Кримінального кодексу України

«Виконання спеціального завдання з попередження чи розкриття кримінально протиправної діяльності організованої групи чи злочинної організації».

Зокрема визначено, що не є кримінальним правопорушенням вимушене заподіяння шкоди правоохоронюваним інтересам особою, яка відповідно до закону виконувала спеціальне завдання, беручи участь в організованій групі чи злочинній організації з метою попередження чи розкриття їх кримінально протиправної діяльності. Така особа, підлягає кримінальній відповідальності лише за вчинення у складі організованої групи чи злочинної організації особливо тяжкого злочину, вчиненого умисно і поєднаного з насильством над потерпілим, або тяжкого злочину, вчиненого умисно і пов'язаного з спричиненням тяжкого тілесного ушкодження потерпілому або настанням інших тяжких або особливо тяжких наслідків. Крім того, передбачено, що особа, яка вчинила такий злочин не може бути засуджена до довічного позбавлення волі, а покарання у виді позбавлення волі не може бути призначене їй на строк, більший, ніж половина максимального строку позбавлення волі, передбаченого законом за цей злочин [3].

Як оперативно-розшуковий захід виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації здійснюється відповідно до положень Закону України «Про оперативно-розшукову діяльність».

Так у стаття 8 вказаного закону підрозділам, які здійснюють оперативно-розшукову діяльність надано право виконувати спеціальне завдання з розкриття злочинної діяльності організованої групи чи злочинної організації згідно з положеннями статті 272 Кримінального процесуального кодексу України. Крім того, статтею 13 визначено, що особа, яка залучається до виконання завдань оперативно-розшукової діяльності, перебуває під захистом держави. Співробітництво особи з оперативним підрозділом зараховується до її загального трудового стажу в разі укладення з нею трудової угоди. Якщо у зв'язку з виконанням такою особою завдань оперативно-розшукової діяльності настала її інвалідність або смерть, на неї поширюються пільги, передбачені у таких випадках для працівників оперативних підрозділів. У разі виникнення загрози життю, здоров'ю або майну особи, яка залучається до виконання завдань оперативно-розшукової діяльності, її захист забезпечується в порядку, передбаченому частиною третьою статті 12 цього Закону України «Про оперативно-розшукову діяльність» [4].

У свою чергу відповідно до положень статті 2 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» право на забезпечення безпеки шляхом застосування заходів, зазначених у статтях 1 і 7 вказаного Закону, за наявності відповідних підстав має особа, яка заявила до правоохоронного органу про кримінальне правопорушення або в іншій формі брала участь чи сприяла виявленню, попередженню, припиненню або розкриттю кримінальних правопорушень [5].

Окремі аспекти виключення матеріальної відповідальності військовослужбовців та деяких інших осіб за шкоду, завдану державному майну, у тому числі військовому майну, майну, залученому під час мобілізації, а також грошовим коштам, під час виконання ними службових обов'язків при виконання спеціального завдання з попередження чи розкриття злочинної діяльності організованої групи чи злочинної організації визначено у Законі України «Про матеріальну відповідальність військовослужбовців та прирівняних до них осіб за шкоду, завдану державі». Так, у статті 9 зазначеного закону визначено, що завдана шкода не підлягає відшкодуванню, а особи звільняються від матеріальної відповідальності у разі, якщо шкоду завдано внаслідок виконання спеціального завдання з попередження чи розкриття злочинної діяльності організованої групи чи злочинної організації [6].

Окремі аспекти виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації визначено у міжвідомчій інструкції «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» від 16 листопада 2012 р. № 114/1042/516/1199/936/1687/5. Зокрема визначено, що виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації полягає в організації слідчим і оперативним підрозділом введення уповноваженої ними особи, яка відповідно до закону виконує спеціальне завдання, в організовану групу чи злочинну організацію під легендою прикриття для отримання речей і документів, відомостей про її структуру, способи і методи злочинної діяльності, які мають значення для розслідування злочину або злочинів, які вчиняються цими групами. Виконання такого завдання здійснюється на підставі постанови слідчого, погодженої з керівником органу досудового розслідування, або постанови прокурора зі збереженням у таємниці достовірних відомостей про особу і не потребує дозволу слідчого судді [7]

Крім того, більшість правоохоронних органів, які у своєму складі мають органи досудового розслідування та/або оперативні підрозділи мають відповідні відомчі нормативні акти в яких визначено особливості виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації. Однак в межах тез неможливо розкрити положення вказаних нормативних актів, оскільки така інформація віднесена до державної таємниці, а такі акти мають відповідний обмежаний доступ.

Підсумовуючи викладене можна дійти до висновку, що відносини, що виникають у процесі виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації на сьогодні регулюється такими нормативно-правовими актами:

– Кримінальний процесуальний кодекс України;

- Кримінальний кодекс України;
- Закон України «Про оперативно-розшукову діяльність»;
- Закон України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві»;
- Закон України «Про матеріальну відповідальність військовослужбовців та прирівняних до них осіб за шкоду, завдану державі»;
- наказ Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України № 114/1042/516/1199/936/1687/5/ від 16.11.2012 «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні»;
- відомчі нормативні акти, які мають обмежаний доступ.

Список використаних джерел:

1. Кудінов С.С., Бачинський О.В. Правове регулювання виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації. Прикарпатський юридичний вісник. 2019. Випуск 4(29). Т 1. С. 183–188.

2. Кримінальний процесуальний кодекс України від 03.04.2012 № 4651-VI. URL: http://www.zakon.rada.gov.ua.html (дата звернення: 25.05.2024).

3. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: http://www.zakon.rada.gov.ua.html (дата звернення: 25.05.2024).

4. Про оперативно-розшукову діяльність: Закон України від 20.12.1990 № 2135-XII. URL: http://www.zakon.rada.gov.ua.html (дата звернення: 25.05.2024).

5. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: Закон України від 23.12.1993 № 3782-XII. URL: http://www.zakon.rada.gov.ua.html (дата звернення: 25.05.2024).

6. Про матеріальну відповідальність військовослужбовців та прирівняних до них осіб за шкоду, завдану державі: Закон України від 03.10.2019 № 160-IX. URL: http://www.zakon.rada.gov.ua.html (дата звернення: 25.05.2024).

7. Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: наказ Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5/. URL: http://www.zakon.rada.gov.ua.html (дата звернення: 25.05.2024).

СЛУЖБА БЕЗПЕКИ УКРАЇНИ В САНКЦІЙНІЙ ПОЛІТИЦІ ДЕРЖАВИ

Сергій НАУМЮК
кандидат юридичних наук, доцент

В умовах збройної агресії з боку російської федерації проти України запровадження санкцій відіграє ключову роль у стримуванні ворожих дій та захисті національних інтересів нашої держави. Ефективність санкційного механізму значною мірою залежить від чіткого правового регулювання та узгодженої взаємодії органів державної влади в цьому процесі. У даному контексті ключова роль відведена Службі безпеки України (далі – СБУ).

Правове підґрунтя санкційної політики закладене в Законі України «Про санкції» від 14.08.2014 № 1644-VII (в редакції від 08.03.2024) [1]. Цей нормативно-правовий акт регулює

правову основу, підстави та принципи застосування спеціальних обмежувальних заходів, а також визначає порядок їх запровадження, внесення змін і скасування.

Окремі аспекти санкційного механізму також регламентуються іншими законодавчими актами, зокрема законами України «Про оборону України», «Про інформацію», «Про основні засади забезпечення кібербезпеки України» та ін.

Згідно з чинним законодавством, СБУ наділена повноваженнями подавати до Ради національної безпеки і оборони України (далі – РНБО) обґрунтовані пропозиції щодо застосування, внесення змін та скасування санкцій. Як свідчить практика, переважна більшість реалізованих на сьогодні санкційних ініціатив були ініційовані саме СБУ [2].

Закон України «Про санкції» передбачає широкий спектр обмежувальних заходів, які можна класифікувати за різними критеріями. На підставі аналізу змісту ст. 4 Закону, пропонуємо поділяти санкції:

1. За характером впливу:

а) Економічні за напрямами:
- фінансові (блокування активів (п. 1), стягнення активів (п. 1–1), зупинення виконання економічних та фінансових зобов'язань (п. 5), заборона вчинення правочинів щодо цінних паперів (п. 12), обмеження фінансових операцій (п. 13, 14, 15));
- торговельні (обмеження торговельних операцій (п. 2), заборона здійснення публічних та оборонних закупівель (п. 10));
- промислові (анулювання чи зупинення дії спеціальних дозволів на користування надрами (п. 6), заборона збільшення розміру статутного капіталу певних господарських товариств (п. 16));

б) Політичні за напрямами:
- дипломатичні (припинення дії міжнародних договорів (п. 22), анулювання офіційних візитів, засідань, переговорів (п. 23));
- візові (відмова в наданні та скасування віз (п. 21), відмова в наданні або скасування дозволу на імміграцію (п. 24–3));

в) Військові за напрямами:
- оборонні (припинення дії спільних проектів та промислових програм у сфері безпеки та оборони (п. 18));
- технологічні (заборона передання технологій, прав на об'єкти права інтелектуальної власності (п. 19));
- логістичні (обмеження, часткове чи повне припинення транзиту ресурсів, польотів та перевезень територією України (п. 3)).

2. За суб'єктом впливу:

а) Проти фізичних осіб за напрямами:
- майнові (блокування та стягнення активів (п. 1, 1–1));
- обмежувальні (заборона в'їзду на територію України (п. 21), примусове повернення або примусове видворення за межі України (п. 24–4));
- статусні (позбавлення державних нагород України, інших форм відзначення (п. 24));

б) Проти юридичних осіб за напрямами:
- економічні (обмеження торговельних операцій (п. 2), заборона участі у приватизації, оренді державного майна (п. 7));
- регуляторні (анулювання або зупинення ліцензій та інших дозволів (п. 6));
- операційні (заборона діяльності на території України (п. 24–2));

в) Проти держави за напрямами:
- дипломатичні (припинення дії міжнародних договорів (п. 22), анулювання офіційних візитів, засідань, переговорів (п. 23));
- економічні (обмеження торговельних операцій (п. 2), припинення дії торговельних угод, спільних проектів та промислових програм (п. 18));

– фінансові (заборона здійснення інвестицій в іноземну державу (п. 13), обмеження валютних операцій (п. 14));
– транспортні (обмеження транзиту, польотів та перевезень (п. 3), заборона або обмеження заходження іноземних суден та повітряних суден (п. 11));
– науково-культурні (припинення культурних обмінів, наукового співробітництва, освітніх та спортивних контактів (п. 20)).

3. За метою:

а) Примусові за напрямами:
– економічні (обмеження торговельних операцій (п. 2), заборона участі у приватизації (п. 7), зупинення виконання економічних та фінансових зобов'язань (п. 5));
– регуляторні (запровадження додаткових заходів у сфері екологічного, санітарного, фітосанітарного та ветеринарного контролю (п. 17));

б) Запобіжні за напрямами:
– економічні (запобігання виведенню капіталів за межі України (п. 4));
– інформаційні (заборона поширення медіа на території України (п. 6–1), заборона користування радіочастотним спектром України (п. 8), обмеження або припинення надання електронних комунікаційних послуг (п. 9));
– технологічні (заборона передання технологій, прав на об'єкти права інтелектуальної власності (п. 19));

в) Каральні за напрямами:
– майнові (блокування та стягнення активів (п. 1, 1–1));
– статусні (позбавлення державних нагород України, інших форм відзначення (п. 24), відмова в наданні та скасування віз (п. 21));
– адміністративні (примусове повернення або примусове видворення за межі України (п. 24–4)).

Наведена класифікація є новаторською спробою структурування обмежувальних заходів за різними критеріями, яка відзначається низкою позитивних рис, що роблять її ефективним інструментом для аналізу та застосування санкційної політики. Насамперед, її багатовимірність, що охоплює три ключові аспекти санкцій – характер впливу, суб'єкт впливу та мету, дозволяє всебічно розглядати кожен санкційний захід. Детальний розподіл кожної категорії на підкатегорії забезпечує глибше розуміння специфіки різних типів санкцій, а логічна ієрархічна структура полегшує сприйняття та аналіз інформації.

Практична цінність цієї класифікації полягає в її потенційній корисності для правників, політологів та економістів при аналізі та розробці санкційної політики. Важливо відзначити, що вона точно відображає зміст статті 4 Закону України «Про санкції», що забезпечує її юридичну релевантність. При цьому, гнучка структура класифікації дозволяє легко доповнювати її новими категоріями або підкатегоріями у разі змін у законодавстві.

Комплексність класифікації виражається в охопленні широкого спектру санкцій – від економічних до військових, від заходів проти фізичних осіб до обмежень для юридичних осіб. Особливо варто відзначити виділення категорії «за метою», що дозволяє краще розуміти інтенції застосування тих чи інших санкцій. Таким чином, ця класифікація надає потужний інструментарій для аналізу, розробки та застосування санкцій, враховуючи їх різноманітні аспекти та потенційні наслідки, що робить її цінним ресурсом у сфері санкційної політики.

Провідна роль СБУ в реалізації санкційної політики полягає в таких ключових аспектах:

1. Збір та аналіз інформації, необхідної для обґрунтування пропозицій щодо застосування чи зміни санкцій. У ролі державного органу спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України, СБУ володіє унікальними можливостями для виявлення загроз національній безпеці та документування відповідних доказів;

2. Ініціювання санкційних процедур. Саме СБУ є основним ініціатором пропозицій щодо запровадження санкцій, які вона подає на розгляд РНБО. Ці пропозиції формулюються на ос-

нові зібраної інформації та проведеного аналізу з урахуванням оцінки потенційних ризиків і наслідків;

3. Експертне та консультативне забезпечення. СБУ, як орган, що забезпечує державну безпеку, має потенціал для надання експертних висновків та консультацій щодо доцільності, обґрунтованості та механізмів реалізації санкційних заходів. Враховуючи специфіку роботи та доступ до інформації з питань національної безпеки, фахівці СБУ мають можливість надавати важливі аналітичні матеріали та рекомендації, які можуть бути використані при формуванні санкційної політики;

4. Забезпечення контролю та моніторингу санкцій. СБУ здійснює моніторинг чинних санкцій, що сприяє підвищенню ефективності контролю за дотриманням санкційної політики та притягненню до відповідальності порушників.

Відповідні функціональні підрозділи СБУ вживають заходи, спрямовані на забезпечення ефективності санкційних заходів. Це включає запобігання спробам суб'єктів, на яких накладено санкції, ухилитися від обмежень, а також протидію зусиллям з перешкоджання впровадженню санкцій. При виявленні недоліків у механізмах реалізації санкцій СБУ надає Кабінету Міністрів України відповідні пропозиції щодо їх усунення для посилення ефективності санкційної політики.

Така активна та різнопланова участь СБУ у санкційному процесі відіграє вирішальну роль у забезпеченні його належної державної організації, обґрунтованості та результативності.

СБУ у своїй діяльності керується основними принципами міжнародного права, що регулюють запровадження обмежувальних заходів. До таких принципів, закріплених у міжнародних договорах та звичаєвих нормах, належать: принцип законності (санкції мають запроваджуватись лише на підставі чинного законодавства та у відповідності зі встановленими процедурами); принцип колективної безпеки (накладення санкцій має узгоджуватись на міжнародному рівні, зокрема через механізми ООН, задля підтримки миру та безпеки); принцип пропорційності (запроваджені заходи не повинні виходити за межі того, що необхідно для досягнення законних цілей санкцій); принцип гуманності (санкції не можуть спричиняти надмірних страждань цивільного населення або порушувати основоположні права людини); принцип недискримінації (застосування обмежувальних заходів має відбуватись рівно та безсторонньо щодо всіх держав та організацій без упередженості; принцип добросовісності (дії держав щодо запровадження санкцій мають бути чесними, прозорими та відповідати принципам справедливості) [3–5].

Аналіз чинного законодавства та міжнародної практики дозволяє виокремити певні проблемні аспекти у сфері застосування санкцій в Україні. Серед них можна назвати:

1. Відсутність детальної регламентації процедури запровадження санкцій. Закон України «Про санкції» має рамковий характер і не містить чітких критеріїв та процедур визначення суб'єктів застосування обмежувальних заходів;

2. Недосконалість нормативно-правового регулювання питань блокування активів осіб, до яких застосовано санкції. Чинне законодавство не передбачає прозорих механізмів виявлення, арешту та подальшого розпорядження майном таких суб'єктів;

3. Непроцесуальний характер Закону України «Про санкції». Відсутність чітких процедур та юридичних наслідків ускладнює правозастосовну практику і створює ризики довільного тлумачення норм права;

4. Недосконалість та фрагментарність санкційного режиму, який проявляється в існуванні численних винятків та обмежень його дії. Це знижує ефективність санкцій та створює можливості для їх обходу.

Наведені проблеми свідчать про необхідність подальшого вдосконалення санкційного законодавства України з метою приведення його у відповідність до міжнародних стандартів і забезпечення ефективного захисту національних інтересів.

Слід визнати, що СБУ відіграє системну та багатоаспектну роль на всіх етапах дій санкційного механізму в Україні.

Внесок СБУ у формування та реалізацію санкційної політики є суттєвим, що підтверджується кількістю і масштабом запропонованих та впроваджених санкційних заходів (82,7%). Діяльність СБУ відіграє вирішальну роль у таких аспектах: як налагодження співробітництва з компетентними органами іноземних держав щодо обміну релевантною інформацією про застосування санкцій; здійснення спільної аналітичної та консультаційної роботи тощо; здійснення безпосереднього контролю за дотриманням санкційних обмежень, а також застосуванням адекватних правових заходів реагування у разі їх порушення; ретельний аналіз і моніторинг ефективності чинних санкційних режимів з метою їх оптимізації та посилення; розробка пропозицій щодо вдосконалення санкційного законодавства та практики його застосування; активна участь у міжвідомчих консультаціях та заходах міжнародного рівня щодо питань, пов'язаних із санкційною політикою.

Список використаних джерел:

1. Про санкції: Закон України від 14.08.2014 р. № 1644-VII: станом на 8 берез. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1644–18#Text (дата звернення: 03.06.2024).

2. Наумюк С. Мета санкційної політики України щодо рф та роль СБ України в цій політиці. Санкції – інструмент безпекової політики держави: зб. матеріалів наук. форуму, м. Київ, 12 верес. 2023 р. Київ, 2023. С. 9–14.

3. Статут Організації Об'єднаних Націй: Статут від 26.06.1945. URL: https://www.un.org/ru/about-us/un-charter/full-text (date of access: 04.06.2024).

4. Задорожна С., Кирилюк Н., Маник А. Загальні принципи в класичному міжнародному праві: від Вестфальського миру до ООН. Юридичний науковий електронний журнал. 2020. № 4. С. 381–385. URL: https://doi.org/10.32782/2524–0374/2020–4/90 (дата звернення: 06.06.2024).

5. Nurullaiev I.S. Basic and general principles of public international law as a source of legal regulation of international cooperation in the fight against crime. State and Regions. Series: Law. 2019. No. 4. P. 218–223. URL: https://doi.org/10.32840/1813–338x-2019–4–36 (дата звернення: 06.06.2024).

СТАН ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КОНТРРОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ В ОСОБЛИВИЙ ПЕРІОД

Євгеній РИБИНСЬКИЙ
доктор філософії в галузі права
співробітник СБУ

Забезпечення національної безпеки України, захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів держави від реальних та потенційних загроз [1] неможливі без організації контррозвідувальної діяльності. У свою чергу, реалізація основних завдань щодо попередження, своєчасного виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України безумовно залежить від належного правового забезпечення контррозвідувальної діяльності, що підтверджує актуальність наукового аналізу правових засад контррозвідувальної діяльності в Україні [2, с. 3].

На сьогодні в Україні організаційні аспекти контррозвідувальної діяльності регламентуються великою кількістю нормативно-правових актів, як на рівні Законів України, так і на відомчому рівні, у тому числі з грифом обмеження доступу.

Можна виділити наступні закони: «Про Службу безпеки України»; «Про контррозвідувальну діяльність»; «Про боротьбу з тероризмом»; «Про державну таємницю»; «Про національну безпеку України»; «Про організаційно-правові основи боротьби з організованою злочинністю»; «Про оперативно-розшукову діяльність»; «Про розвідку» та ін.

Зокрема, в Законі України «Про контррозвідувальну діяльність» визначено поняття, мету і завдання контррозвідувальної діяльності; її правову основу та принципи на яких вона ґрунтується; перелік суб'єктів, яким надано право здійснювати контррозвідувальну діяльність; підстави для проведення контррозвідувальної діяльності; він закріплює функції і повноваження органів, підрозділів та співробітників Служби безпеки України, що здійснюють контррозвідувальну діяльність; основні засади організації контррозвідувальної діяльності; регламентує питання захисту відомостей про контррозвідувальну діяльність; окреслює соціальні та правові гарантії співробітників органів і підрозділів Служби безпеки України, які здійснюють контррозвідувальну діяльність; встановлює гарантії дотримання законності під час здійснення контррозвідувальної діяльності, а також регулює питання контролю за контррозвідувальною діяльністю, нагляду за дотриманням законності органами та підрозділами, що її здійснюють [3].

Метою контррозвідувальної діяльності є попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення [3].

Основними завданнями контррозвідувальної діяльності є: добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; протидія розвідувальній, терористичній та іншій діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян [3].

Законом України «Про контррозвідувальну діяльність» визначено, що спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності є Служба безпеки України. При цьому, організація та координація контррозвідувальної діяльності покладаються на Центральне управління Служби безпеки України.

Разом із тим, контррозвідувальні заходи в інтересах забезпечення охорони державного кордону України, посадових осіб, стосовно яких здійснюється державна охорона, можуть проводити розвідувальні органи України, підрозділи забезпечення внутрішньої і власної безпеки Державної прикордонної служби України та Управління державної охорони України, яким законами України надано право здійснювати оперативно-розшукову чи розвідувальну діяльність. У свою чергу, розвідувальні органи України також можуть проводити контррозвідувальні заходи у випадках, зазначених у статті 17 Закону України «Про розвідку» [4].

Також відповідно до Закону України «Про оперативно-розшукову діяльність» оперативні підрозділи під час здійснення оперативно-розшукової діяльності можуть проводити контррозвідувальні заходи [5].

Здійснення контррозвідувальних заходів іншими суб'єктами забороняється.

В Україні контррозвідувальна діяльність здійснюється гласно і негласно. Гласні контррозвідувальні заходи передбачають використання відкритих (офіційних) форм і методів роботи у сфері забезпечення державної безпеки. У свою чергу, негласні контррозвідувальні заходи здійснюються із залученням осіб, які негласно (конфіденційно) співпрацюють з органами і підрозділами, що можуть здійснювати контррозвідувальну діяльність, а також з використанням оперативних, оперативно-технічних та спеціальних сил і засобів [6, с. 259].

При цьому, відомості про організацію, плани, зміст, форми, методи, засоби, фінансування та матеріально-технічне забезпечення, результати контррозвідувальної діяльності, наукових і науково-технічних розробок з питань забезпечення державної безпеки, а також про осіб, які

співробітничають або раніше співробітничали на конфіденційній основі з органами та підрозділами Служби безпеки України, що здійснюють контррозвідувальну діяльність, узагальнюючі відомості про особовий склад цих органів та підрозділів становлять державну таємницю і підлягають захисту в порядку, визначеному чинним законодавством [3].

Слід зазначити, що на сьогодні, в умовах повномасштабного вторгнення країни-агресора, Верховною радою України прийнято до розгляду цілу низку законопроектів щодо внесення змін та доповнень до Закону України «Про контррозвідувальну діяльність». Мова йде про основний та альтернативний проекти – «Про внесення змін до деяких законодавчих актів України щодо удосконалення організаційно-правових засад здійснення контррозвідувального забезпечення Збройних Сил України та інших військових формувань, утворених відповідно до законів України» (проект від 08.04.2022 р. № 7267; основний) [7] та «Про внесення змін до деяких законодавчих актів України щодо удосконалення правових основ організації та здійснення контррозвідувальної діяльності в Україні» (проект від 25.04.2022 № 7267–1; альтернативний) [8].

Можна також вказати Проект Закону України «Про внесення змін до деяких законів України щодо удосконалення організаційно-правових засад розвідувальної та контррозвідувальної діяльності» (проект Закону України від 17.05.2022 № 7380) [9], а також на два законопроекти: «Про внесення змін до деяких законодавчих актів України щодо посилення спроможності суб'єктів контррозвідувальної діяльності у протидії широкомасштабній військовій агресії Російської Федерації проти України» (проект Закону України від 19.08.2022 № 7684; основний) [10] та «Про внесення змін до деяких законів України щодо удосконалення контррозвідувальної діяльності та посилення інституційної спроможності суб'єктів її здійснення під час відсічі збройній агресії проти України» (проект Закону України від 05.09.2022 № 7684–1; альтернативний) [11].

Зауважимо, що, на відміну від чинного Закону України «Про контррозвідувальну діяльність» та, наприклад, Закону України «Про оперативно-розшукову діяльність», вказані проекти містять визначення «контррозвідувального заходу», під яким пропонується розуміти рішення та дії суб'єкта контррозвідувальної діяльності, спрямовані на вирішення визначених законом завдань, що реалізується силами контррозвідки із застосуванням методів і засобів контррозвідки стосовно осіб і об'єктів, що становлять чи створюють загрози державній безпеці України або підвищують ризики державної безпеки, незалежно від правового статусу та місця знаходження (діяльності) таких осіб і об'єктів [7; 8]. Визначено засоби контррозвідки – це засоби та структури прикриття, будівлі, приміщення, транспортні засоби, інформаційні системи та бази даних, спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації, озброєння, боєприпаси, військова та спеціальна техніка, інше майно, кошти в національній та іноземних валютах, які використовуються для здійснення контррозвідувальної діяльності (проведення контррозвідувальних заходів) або для організації чи забезпечення її (їх) здійснення (проведення) [7].

Аналізуючи правові засади контррозвідувальної діяльності в Україні, необхідно наголосити, що у вказаних проектах вперше пропонується на законодавчому рівні закріпити такі поняття, як «ризик державної безпеки», «управління ризиками державної безпеки», «контррозвідувальне забезпечення», «контррозвідувальна операція», «контррозвідувальний режим», «пошуковий захід» та «спеціальна інформаційна операція». На нашу думку, доповнення законодавчого тезаурусу цими поняттями сприятиме більш повному розумінню норм закону.

Слід зазначити, що положення та пропозиції, передбачені розглянутими законопроектами, за нашим переконанням, відповідають викликам сьогодення та сприятимуть вдосконаленню правового забезпечення контррозвідувальної діяльності в Україні.

Список використаних джерел:

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Верховна Рада України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2469–19/print. (дата звернення: 15.06.2024)

2. Албул С.В. Правові засади контррозвідувальної діяльності в Україні. Південноукраїнський правничий часопис. 2023. № 2. С. 3–7.

3. Про контррозвідувальну діяльність: Закон України від 26 грудня 2002 року № 374-IV. Редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/374–15#Text. (дата звернення: 15.06.2024)

4. Про розвідку: Закон України від 17 вересня 2020 року № 912-IX. Редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/912–20#Text. (дата звернення: 15.06.2024)

5. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. Редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2135–12#Text. (дата звернення: 15.06.2024)

6. Ватраль А.В. Методологія контррозвідувального пізнання. Науковий вісник публічного та приватного права. 2017. Випуск 4. С. 258–262.

7. Про внесення змін до деяких законодавчих актів України щодо удосконалення організаційно-правових засад здійснення контррозвідувального забезпечення Збройних Сил України та інших військових формувань, утворених відповідно до законів України: проєкт Закону України від 08.04.2022 р. № 7267. Верховна Рада України. Офіційний вебпортал парламенту України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=74070. (дата звернення: 15.06.2024)

8. Про внесення змін до деяких законодавчих актів України щодо удосконалення правових основ організації та здійснення контррозвідувальної діяльності в Україні: проєкт Закону України від 25.04.2022 № 7267–1. Верховна Рада України. Офіційний вебпортал парламенту України. URL: http://w1.c1.rada. gov.ua/pls/zweb2/webproc4_1?pf3511=74143. (дата звернення: 15.06.2024)

9. Про внесення змін до деяких законів України щодо удосконалення організаційно-правових засад розвідувальної та контррозвідувальної діяльності: проект Закону України від 17.05.2022 № 7380. Верховна Рада України. Офіційний вебпортал парламенту України. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/39613. (дата звернення: 15.06.2024)

10. Про внесення змін до деяких законодавчих актів України щодо посилення спроможності суб'єктів контррозвідувальної діяльності у протидії широкомасштабній військовій агресії Російської Федерації проти України: проект Закону України від 19.08.2022 № 7684. Верховна Рада України. Офіційний вебпортал парламенту України. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40270. (дата звернення: 15.06.2024)

11. Про внесення змін до деяких законів України щодо удосконалення контррозвідувальної діяльності та посилення інституційної спроможності суб'єктів її здійснення під час відсічі збройній агресії проти України: проект Закону України від 05.09.2022 № 7684–1. Верховна Рада України. Офіційний вебпортал парламенту України. URL: https://itd.rada.gov.ua/billInfo/Bills/searchResults. (дата звернення: 15.06.2024).

ПРОВЕДЕННЯ ФІНАНСОВИХ РОЗСЛІДУВАНЬ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ТЕРОРИСТИЧНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Максим СОКОЛОВСЬКИЙ
доцент Національного юридичного університету
імені Ярослава Мудрого

Фінансові розслідування під час досудового розслідування терористичних кримінальних правопорушень є важливим елементом у боротьбі з тероризмом. Вони зосереджені на виявленні та блокуванні фінансових потоків, що забезпечують терористичну діяльність. Зазначені розслідування включають комплекс спеціалізованих методів і заходів, які допомагають виявити джерела фінансування тероризму та притягнути до відповідальності осіб, причетних до їх

фінансування. Слід зазначити, що протидія тероризму одне з головних завдань СБ України та є особливо актуальним в сучасних умовах повномасштабного вторгнення рф та існування в Україні тимчасово окупованих територій.

Згідно звіту FATF Ризики фінансування тероризму від 2015 року та аналізу фінансових документів різних терористичних організацій (далі -ТО), показує, що фінансове управління є особливо важливим для терористичних угруповань. Великі ТО нерідко використовують послуги фінансових керуючих для акумулювання доходів, створення захисних фінансових структур, контролю за використанням фінансових коштів тощо.

Так, ТО можуть використовують кошти на наступні цілі:

– проведення терористичних операцій та актів. Це включає витрати на поїздки в місця проведення терористичних атак, а також придбання зброї (у тому числі саморобних вибухових пристроїв), фальшивих документів, витрати, пов'язані з проживанням, харчуванням та лікуванням тощо. Вказані витрати притаманні і для терористів-одинак;
– пропаганда і вербування нових членів ТО. Багато ТО використовують соціальні мережі для звернення до своїх прихильників робити грошові пожертвування, а розвиненіші ТО вкладають гроші у придбання телевізійних і радіостанцій, журналів і газет, доменних імен в Інтернеті та адміністрування веб-сайтів для поширення своїх поглядів. Недопущення ведення пропаганди тероризму стало одним з пріоритетних напрямків боротьби з тероризмом;
– навчання і підготовка своїх співучасників. Наприклад, володіння зброєю, виготовлення вибухових пристроїв, використання таємних засобів зв'язку тощо. Для цього ТО часто купують будинки та ділянки землі для облаштування на них тренувальних таборів. Для охоплення ширшого кола осіб проводиться віртуальне навчання через Інтернет;
– виплата грошового утримання і компенсацій керівництву і членам. У тому числі здійснюються виплати або довгострокові фінансові підтримки сім'ям заарештованих або загиблих бойовиків;
– соціальна підтримка населення. З метою підриву довіри до законних урядів, а також для завоювання підтримки місцевого населення і сприяння вербування нових членів з боку ТО здійснюється фінансування соціальних установ, що надають медичні, соціальні та освітні послуги, які не може забезпечити держава.

Згідно Рекомендацій 30 FATF термін «фінансове розслідування» означає дослідження фінансових відносин, пов'язаних зі злочинною діяльністю з метою:

– встановлення обсягу злочинних мереж та/чи рівня злочинності;
– встановлення та відстеження злочинних доходів, коштів терористів чи будь-яких інших активів, які підлягають, чи можуть підлягати конфіскації;
– представлення доказів, які можуть бути використані при кримінальному переслідуванні.

Таким чином, фінансове розслідування це дослідження фінансових аспектів злочинної діяльності, у тому числі шляхом проведення комплексу аналітичних та слідчих (розшукових) дій, спрямованих на здобуття доказів для використання у кримінальному судочинстві, що вказують на злочинну діяльність, ідентифікують прибутки від такої діяльності та джерела фінансування злочинної діяльності.

Іншими словами можна сказати, що це пошук слідів злочину (у тому числі у сфері терористичних кримінальних правопорушень) через фінансові відносини. Слід зазначити, що Рекомендація 30 FATF закликає країни призначати слідчих у кримінальних справах для розслідування злочинів у сфері тероризму. Новий напрямок включає необхідність проведення паралельних фінансових розслідувань.

Паралельне фінансове розслідування означає одночасне використання інструменту фінансових розслідувань у разі досудового розслідування у межах одного провадження вчинення терористичного акту та фінансування тероризму. Рекомендація 30 FATF вказує, що відносно будь-якого злочину, пов'язаного з фінансуванням тероризму, правоохоронним органам необхідно ініціативно проводити паралельне фінансове розслідування. При проведенні паралель-

ного розслідування досвід і знання з різних сфер розслідування доповнюють один одного, що сприяє більш повному розслідуванню злочинів.

Таким чином, проведення фінансових розслідувань, яке включає, зокрема, відстеження злочинних активів, їх арешт та конфіскацію, дає можливість:

– позбавлення терористів доходу від протиправної діяльності та, як наслідок, позбавлення мотивації до вчинення нових злочинів;
– виявлення терористичних організацій та її членів;
– позбавлення злочинців можливості продовжувати та розвивати терористичну діяльність (виявлення злочинних схем і зв'язків, ключових фігурантів, позбавлення терористичних організацій фінансування);
– виявлення інших кримінальних злочинів (які були раніше невідомі) та інших активів (які можна у подальшому конфіскувати);
– відшкодування збитків потерпілим та державі

Так, порядок ведення фінансового розслідування у Швеції передбачає проведення спрощеного та поглибленого майнового розслідування. Спрощене майнове розслідування може включати аналіз наступних даних:

– дані Реєстру населення Швеції;
– відкрита інформація з оподаткування за минулі 10 років;
– дані щодо (прав) володіння нерухомим майном;
– боргові вимоги, передані до виконання Службі судових приставів;
– участь у керуванні компаніями;
– дані щодо (прав) володіння транспортними засобами;
– виписки з рахунків;
– відомості про іпотечні займи та їх забезпечення тощо.

Спрощене розслідування завершується складанням узагальненої довідки щодо отриманих даних та направленням рекомендацією слідчого, в якій він пропонує прокуратурі вжити певні подальші слідчі заходи. У ході діалогу між прокуратурою та слідчим також розглядається, які види конфіскації можуть бути застосовані, виходячи з існуючих підозр і результатів спрощеного аналізу активів.

Якщо спрощене розслідування дасть підстави для подальших слідчих заходів щодо економічної діяльності підозрюваного, то наступним кроком буде так зване поглиблене майнове розслідування (аналіз активів), яке включає:

– допит підозрюваних осіб;
– проведення оперативно-технічних або негласно слідчих розшукових заходів;
– збір додаткових банківських даних та аналіз грошових потоків;
– з'ясування майнових відносин і прав власності на активи, оформлені на підставних осіб;
– підрахунок незаконних доходів тощо.

Одним з перших кроків у фінансових розслідуваннях є аналіз банківських рахунків та фінансових транзакцій. Слідчі або оперативні співробітники зосереджуються на виявленні підозрілих операцій, які можуть свідчити про фінансування терористичної діяльності. Це включає вивчення великих, незвичайних або регулярних сум, а також аналіз походження коштів, що надходять на рахунки підозрюваних осіб чи організацій.

Крім традиційних банківських рахунків, особлива увага приділяється електронним гаманцям та криптовалютам. Зростання використання криптовалют у фінансуванні тероризму вимагає аналізу блокчейн-транзакцій для відстеження руху коштів. Також аналізуються фінансові звіти підприємств і благодійних організацій, які можуть використовуватися для приховування терористичних фінансів.

Фінансові розслідування зосереджуються на виявленні як легальних, так і нелегальних джерел доходу, що використовуються для фінансування ТО. Це включає перевірку благодійних організацій на предмет використання їх для збору коштів на терористичну діяльність під виглядом законної діяльності. Також розслідуються доходи від незаконної торгівлі, контрабанди, торгівлі наркотиками та іншої злочинної діяльності.

Однією з важливих задач є ідентифікація фінансових посередників, які переводять кошти від донорів до терористичних груп. Аналізуються фінансові операції близьких родичів та друзів підозрюваних осіб, щоб виявити можливі зв'язки з терористичними організаціями.

Для успішного проведення фінансових розслідувань важливо співпрацювати з державними вітчизняними та міжнародними установами. Слід зазначити, що під час досудового розслідування терористичних кримінальних правопорушень доцільним є звернення до наступних органів щодо допомоги у відстеженні руху коштів чи майна:

– Державна служба фінансового моніторингу України;
– Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів;
– Державна податкова служба України;
– Державна аудиторська служба України;
– Антимонопольний комітет України;
– Державна митна служба України.

Фінансові розслідування терористичних правопорушень часто вимагають міжнародного співробітництва. Використання каналів Інтерполу та Європолу для обміну інформацією про фінансові операції терористичних організацій є важливим аспектом таких розслідувань. Крім того, слідчі та оперативні співробітники взаємодіють з національними фінансовими розвідувальними підрозділами та міжнародними організаціями, для координації зусиль у боротьбі з фінансуванням тероризму, такими як:

– FATF – міжурядовий орган, метою роботи якого є розвиток і впровадження на міжнародному рівні заходів і стандартів з боротьби щодо відмивання грошей та протидія фінансуванню тероризму;
– Egmont Group – неформальне об'єднання підрозділів фінансових розвідок;
– Камденська міжвідомча мережа з повернення активів (CARIN) – це неформальна мережа представників правоохоронних органів і судових практиків, фахівців в області виявлення та розшуку активів, заморожування, арешту та їх конфіскації.

Міжнародні договори та меморандуми про взаєморозуміння полегшують обмін інформацією та координацію зусиль у розслідуванні фінансування тероризму. Використання механізмів міжнародної правової допомоги дозволяє отримувати докази та проводити розслідування за кордоном.

Одним з ключових завдань фінансових розслідувань є виявлення та блокування активів, які можуть використовуватися для фінансування терористичної діяльності. Це включає замороження банківських рахунків та інших фінансових активів підозрюваних осіб та організацій, а також проведення процедур з конфіскації майна. Доречним також є використання можливостей Держфінмоніторингу щодо зупинення проведення видаткових операцій на рахунках, що сприятиме арешту незаконно здобутих доходів та забезпечення спеціальної конфіскації.

Важливу роль відіграє співпраця з іноземними урядами для замороження активів, розташованих за межами країни, а також використання міжнародних санкційних списків для ідентифікації та блокування активів терористів.

З рахуванням викладеного, можливо виділити наступні переваги проведення фінансових розслідувань терористичних кримінальних правопорушень:

– встановлення додаткових доказів, свідків, співучасників або жертв;
– виявлення мотивів, цілей та притягнення до відповідальності організаторів та співучасників терористичної організації;
– встановлення додаткових інструментів вчинення злочину (телефон, транспорт, платіжні інструменти (криптовалюти, електронні гроші тощо);
– відслідковування злочинних активів, їх арешт та конфіскація з метою відшкодування збитків потерпілим та державі;
– виявлення інших кримінальних злочинів (які були раніше невідомі) та інших активів (які можна у подальшому конфіскувати) тощо.

Таким чином, фінансові розслідування відіграють значну роль у виявленні та запобіганні терористичних кримінальних правопорушень, оскільки вони дозволяють розкрити фінансові мережі, які підтримують терористичну діяльність, і притягнути до відповідальності осіб, причетних до їх фінансування.

Враховуючи, що протидія тероризму одне з головних завдань СБ України та є особливо актуальним в сучасних умовах повномасштабного вторгнення рф, а також взяті Україною на себе зобов'язання та необхідність впровадження у національну правову систему сучасних, інноваційних засобів здійснення досудового розслідування, вважається за доцільним, що питання стосовно фінансового розслідування (у тому числі паралельного) потребує широкого обговорення юридичною громадськістю та узагальнення досвіду розвинених держав. Також існує необхідність у всебічному вивченні зарубіжного досвіду у розробленні механізмів фінансових розслідувань та їх запровадженні у вітчизняну практику.

Список використаних джерел:

1. Міжнародні стандарти з протидії відмиванню доходів та фінансуванню тероризму і розповсюдженню зброї масового знищення.– Рекомендації FATF, 2018 URL: https://www.mof.gov.ua/storage/files/Рекомендац_.pdf (дата звернення: 12.06.2024).

2. Ризики фінансування тероризму – Звіт FATF, 2015 URL: https://www.fiu.gov.ua/content/file/Site_docs/2016/20160727/Zmist1.pdf (дата звернення: 12.06.2024).

УДОСКОНАЛЕННЯ ІНСТРУМЕНТАРІЮ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Олег ТАРАСЕНКО
доктор юридичних наук, професор
співробітник МВС

Починаючи з 2014 року, коли рф розпочала активну фазу гібридної війни проти України, ворог використовував кіберпростір для проведення хакерських атак, поширення фейків, проведення нформаційних спецоперацій. З початку збройного вторгнення до цього переліку додалися ряд злочинних дій, які пов'язані з кібертероризмом і кібершпигунством – такий арсенал сьогодні застосовують російські спецслужби. СБУ ефективно забезпечує інформаційну безпеку держави – тільки за 2022 рік СБУ нейтралізувала майже 4,5 тисячі кібератак і кіберінцидентів, метою яких є дестабілізація ситуації в Україні, послаблення міжнародної підтримки України [1, С. 8]. При цьому спецслужби рф постійно удосконалюють технічні й програмні засоби для полегшення вчинення зазначених кібератак – тобто переваги сучасного цифрового світу та розвиток інформаційних технологій обумовив виникнення нових загроз національній безпеці [2, С. 42]. В таких умовах особливого значення набуває пошук нових можливостей активної протидії, своєчасного виявлення ознак кібератак. Аналіз стану інформаційної безпеки в режимі реального часу та оперативно реагування на будь-які кіберзагрози є одним з першочергових завдань СБУ. Виконання зазначеного завдання потребує використання відповідного інструментарію.

У цьому сенсі необхідно відмітити систему Securityi2Analyst'sNotebook від компанії IBM [3] – це інструмент візуального аналізу, що допомагає перетворити дані в осмислену (графічну) інформацію. Рішення включає інноваційні функції, такі як візуалізація взаємопов'язаних мереж, аналіз соціальних мереж, просторові й тимчасові уявлення, які дозволяють виявляти приховані зв'язки і закономірності в даних. Застосування Securityi2Analyst'sNotebook надає можливість супроводжувати та підтримувати оперативно-розшукову діяльність (упорядкуван-

ня інформації, її оцінка, представлення результатів аналізу, пошук інформації з власних баз тощо) при цьому вказана система здатна автоматично проаналізувати накопичені дані, розплутувати складні зв'язки в мережах, що відображають взаємодію об'єктів різної природи. Так, під час здійснення аналізу телефонних роздруківок використання Securityi2Analyst'sNotebook дозволяє: перевірити, підтвердити чи спростувати робочі оперативні версії; визначити ймовірну роль участі контактів при вчиненні протиправної діяльності; встановити зв'язки з особами, які раніше потрапляли у поле зору; визначити місця імовірного проживання об'єктів аналізу, їх спільних контактів; установлення інших телефонних трубок і карток, що використовуються об'єктами, особливостей їх використання; визначення нових об'єктів, які доцільно взяти до уваги при здійсненні оперативно-розшукової діяльності, тощо [4, С. 70]. Необхідно зауважити, що програма IBMi2Analyst'sNotebook (та інші подібні аналітичні продукти, які здебільшого використовуються в діяльності правоохоронних органів), має обмежені можливості в питанні об'єму інформації, що обробляється та аналізується. Тому для таких завдань – обробки та аналізу великого масиву даних, а також отримання інформації з мережі Інтернет – аналітики використовують спеціально створені для виконання таких завдань мови програмування, на кшталт Python. Варто відмітити, що можливо використовувати й інші мови програмування, але Python є найбільш придатною за функціоналом та легкістю розуміння мовою програмування саме для аналізу великого масиву даних та веб-скрапінгу(або парсинг) [5, С. 5]. Окрім аналізу даних та вебскрапінгу за допомогою мови програмування Python також можливо отримувати інформацію з APIвеб-сайтів. Прикладний програмний інтерфейс (англ. ApplicationProg rammingInterface, скорочено API) – це сукупність засобів та правил, що вможливлюють взаємодію між окремими складниками програмного забезпечення або між програмним та апаратним забезпеченням. Простими словами – це спеціальний алгоритм, який дозволяє власникам вебсайтів автоматично завантажувати інформацію. В розумінні теорії відкритих даних API надає можливість користувачу отримувати дані від володільців вебсайтів, які добровільно надали згоду на отримання та обробку таких даних. Наприклад, такі іноземні вебсайти, як Facebook, Twitter, Reddit тощо, а також низка вітчизняних вебсайтів (www.data.gov.ua, www.spending.gov.ua, www.rada.gov.ua тощо) пропонують кожному користувачу мережі Інтернет API для завантаження даних з їхніх веб-сайтів. Головною перевагою даних отриманих з API – це зручний формат обробки та аналізу таких даних. Тобто це використання форматів даних, які придатні для автоматизованої обробки її засобами обчислювальної техніки. Як правило, це такі формати, як CSV, XML, JSON, RDFa, HTMLMicrodatatощо. Суть роботи з API полягає в надсиланні за допомогою мови програмування запиту на отримання інформації та миттєвого отримання відповіді від вебсервера. Перевагою використання API є: можливість отримувати актуальні дані в автоматичному режимі без необхідності кожен раз завантажувати оновлений набір даних; можливість обирати конкретний тип даних (наприклад, тільки коментарі користувачів соціальних мереж), що дає можливість не завантажувати великі об'єми даних; можливість створення власних програм, в тому числі аналітичних, для виконання конкретних завдань. Саме мова програмування Python дозволяє повноцінно використовувати всі переваги APIвебсайтів. Для того, щоб правильно інсталювати, використовувати мову програмування Python для здобуття інформації в мережі Інтернет та зрозуміти всі її переваги необхідно визначити поняття та надати основи, характерні ознаки даної мови програмування [5, С. 5–6].

Поряд з вказаними пошуковими програмами (системами) науковці пропонують використовувати програмне забезпечення, яке було розроблене) з метою протидії відмиванню грошей, корупції та іншим видам організованої злочинності, але може бути використано з метою виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту у мережі Інтернет[6]. Пропонується наступне програмне забезпечення: goAML (збір та аналіз інформації про фінансові операції та угоди); goPRS(підозрілі операції та угоди); goCASE (аналіз інформації, отриманої у ході оперативних і досудових розслідувань); goTRACE (оперативний обмін зашифрованими даними конфіденційного характеру, виявлення зв'язків між особами, адресами і контактними даними) [7].

Використання зазначеного інструментарію дозволить ефективніше протидіяти кіберзагрозам, які створюються спецслужбами рф у ході збройної агресії проти України.

Список використаних джерел:

1. Гора І.В., Колесник В.А., Малюк В.В. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: моногр.; за заг. ред. В.А. Колесника. К.: «7БЦ», 2023. 512 с.

2. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. К.: Видавничий дім «АртЕк». 2017. С. 42.

3. IBM Security i2 Analyst's Notebook. https://www.ibm.com/ru-ru/products/i2-analysts-notebook.

4. Кіревич О.С. Використання альтернативних аналітичних інструментів у кримінальному аналізі. Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки / за ред. Б.М. Олексієнка. Хмельницький, 2016. № 4 (70). С. 70.

5. Школьніков В.І., Орлов Ю.Ю., Корнейко О.В., Вознюк А.А. Здобуття доказової інформації в мережі Інтернет із використанням можливостей мови програмування Python: метод. рек. К.: Нац. акад. внутр. справ, 2020. С. 5.

6. Тарасенко О.С. Використання пошукових програм (систем) підрозділами Національної поліції під час виявлення протиправного контенту.Становлення та розвиток наукових досліджень: матеріали І Міжнар. наук.– практ. конф., присвяченої Дню науки України (м. Київ, 20–21 трав. 2016 р.). Київ: ГО «Фундація науковців та освітян», 2016. С. 81 85.;

7. Кржечковськис І., Тацієнко В.В., Стрільців О.М. та ін.Європейський досвід протидії корупції: теорія та практика: аналіт. огляд.К.: Нац. акад. внутр. справ, 2016. 170 с.

ВИКОРИСТАННЯ КОНТЕНТ-АНАЛІЗУ ЯК МЕТОДУ ПОШУКОВОЇ ДІЯЛЬНОСТІ У ПРОЦЕСІ ВИЯВЛЕННЯ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ

Володимир ФІЛОНОВ
здобувач Науково-дослідного
інституту публічного права

Колабораційна діяльність здійснюється у різних формах, частина з яких передбачає використання засобів масової інформації, соціальних мереж, інших місць публічного розповсюдження інформації. Наприклад, публічні заклики (де заклики – спроби активного впливу, тобто усно, із використанням технічних засобів, пристосованих до передання вербальної інформації на невизначену кількість людей) до: співпраці, підтримки рішень, дій держави-агресора, збройних формувань держави-агресора, окупаційної адміністрації держави-агресора, невизнання поширення державного суверенітету України на тимчасово окуповані території України; до проведення незаконних виборів та/або референдумів до незаконних органів влади, створених на тимчасово окупованій території, публічне заперечення (де заперечення – невизнання окремих фактів чи подій): здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України; здійснення інформаційної діяльності, а саме створення, збирання, одержання, зберігання, використання та поширення антиукраїнської інформації (у співпраці з державою-агресором та/або його окупаційною адміністрацією).

Тому у процесі виявлення зазначених дій ефективним є застосування інформаційного пошуку у всіх джерелах, де може бути розповсюджена зазначена вище інформація. В рамках цьо-

го методу здійснюється пошук та отримання інформації загального користування з телекомунікаційних мереж та інформаційних систем (доступ до яких не обмежується власником або володільцем) про інформаційну антиукраїнську діяльність певних осіб. Але для здійснення такого пошуку необхідно застосування певної методики, що дозволить вичленувати конкретні факти зазначеної колаборaційної інформаційної діяльності зі всього неструктурованого масиву розрізненої інформації, яка міститься в інформаційному просторі.

З врахуванням зазначених вимог – найбільш доцільним є застосування контент-аналізу отримуваних відомостей з метою виявлення тенденцій, які вказують на можливу колаборaційну діяльність певних осіб. Зазначений метод ґрунтується на класичній «репрезентативній» моделі мови, згідно з якою ознаки (слова та символи) репрезентують, тобто виражають, цілком певні значення, що однаково прочитуються, а зв'язки між знаком і значенням є досить стійкими. Для текстів масової комунікації досить характерні загальна доступність значень і загальноприйнятність символів. Отже, в потоці масової інформації циркулюють фрагменти змісту, які завдяки повторюваності необхідно виділити та зафіксувати. Все це й обумовлює доцільність використання контент-аналізу, оскільки він, власне, і передбачає додержання принципу регулярного, ретельного, формалізованого дослідження фрагментів змісту у повідомленнях ЗМІ та інших публічних – інформаційних повідомленнях. Практично, механізм пошуку, що проводяться методом контент-аналізу, полягає у відшуканні індикаторів, які вказують на наявність в документі значущої для аналізу теми, що розкриває зміст текстової інформації, що у нашому випадку обумовлює необхідність встановлення у текстах інформаційних повідомлень (які зроблені і авторизовані як належні певній особі) наявності ознак зазначених вище форм колаборaційної діяльності.

Під час здійснення аналізу певних проблем, змістовні одиниці можуть включати: внутрішні і зовнішні події, осіб та авторів, які описують ці події, або є їх ініціаторами чи учасниками; ставлення до явищ, що відбуваються (їх оцінка), в термінах (поняттях)»за – проти», «вигідно – невигідно», «добре – погано», в чиїх інтересах виникають описувані події або явища, наскільки вони доцільні і таке інше; цільову установку діяльності громадських організацій, рухів, політичних партій, об'єднань та їх діячів, окремих осіб; інтереси (політичні, економічні, партійні, особисті), що має на меті об'єкт дослідження; сам об'єкт спрямованої дії (конкретні гасла, програми, цілі); засоби досягнення кінцевої мети (переконання, насильство, «економічний тиск», моральний чи політичний вплив); характер авторитетів, що залучаються до аргументації поставленої мети (певні політичні діячі, організації, масові видання, логічні висновки, емоційні стереотипи тощо) [1]. Вивчення думок науковців, які розроблювали проблематику контент-аналізу [2, с. 172–178] дає змогу визначити його тактичні прийоми, що найбільш доцільні у процесі виявлення ознак колаборaційної діяльності, а саме: аналіз по елементах (полягає в класифікації окремих часток матеріалів у ЗМІ); тематичний аналіз (дозволяє виявляти явний та прихований зміст, поданий у контексті з іншими повідомленнями або подіями); структурний аналіз (ґрунтується на взаємовідносинах різних тем у ЗМІ); оперативний контент-аналіз (передбачає здійснення аналізу з врахуванням інформації, отриманої з інших (у тому числі негласних) джерел).

Список використаних джерел:

1. Ньюман Л. Неопросні методи дослідження. Соціологічні дослідження. 1998. № 6. С. 119–129.

2. Осадчий Д.О. Ескалація інформаційних загроз національним інтересам України з боку російських ЗМІ. Економіко-правові проблеми становлення в Україні громадянського суспільства: Зб. наук.– метод. праць. Херсон, 2002. С. 172–178.

ДО ПРОБЛЕМ КОНТРРОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Сергій ХАЛИМОН
доктор юридичних наук, професор,
Національна академія Державної
прикордонної служби України
імені Богдана Хмельницького

Відповідно до п. 10 ч. 1 ст. 19 Закону України «Про державну прикордонну службу України» Держприкордонслужба наділена повноваженнями здійснювати контррозвідувальні заходи в інтересах забезпечення охорони та захисту державного кордону України [1], а саме: має право здійснювати окремі контррозвідувальні заходи винятково в інтересах забезпечення охорони державного кордону України, забезпечення безпеки своїх сил і засобів, інформаційних систем та оперативних обліків. Проте вказані положення не деталізували суб'єктів здійснення такої діяльності до певного часу.

Російська агресія 2014 року, Антитерористична операція, а потім операція Об'єднаних сил вимагали розширення переліку суб'єктів здійснення контррозвідувального забезпечення сил оборони. У 2016 році до ст. 5 Закону України «Про контррозвідувальну діяльність» включено положення, що контррозвідувальні заходи в інтересах забезпечення охорони державного кордону України можуть проводити розвідувальні органи України, підрозділи забезпечення внутрішньої і власної безпеки Держприкордонслужби, яким законами України «Про оперативно-розшукову діяльність» та «Про розвідку» надано право здійснювати оперативно-розшукову чи розвідувальну діяльність [2]. Отже, підрозділи забезпечення внутрішньої та власної безпеки Держприкордонслужби (далі – ВВБ) набули повноважень контррозвідувального органу.

У спеціальній літературі з проблем контррозвідувальної діяльності поширена теза, що «контррозвідка ніколи не була такою актуальною, як сьогодні» [3, с. 2], проте вона має безпосереднє відношення до трагічних подій 11 вересня 2001 року в США. Сьогодні ця теза є актуальною для подій в Україні, можна з впевненістю стверджувати, що контррозвідувальна діяльність для Держприкордонслужби ніколи не була такою актуальною як зараз. До повномасштабного вторгнення цей напрямок діяльності лише набирав своїх обертів і, відверто кажучи, до певної міри не приносив результату. Основна робота спрямовувалася на протидію і запобігання кримінальним та іншим правопорушенням, що вчинялися особовим складом Держприкордонслужби. Очевидним є те, що ніхто не вірив у повномасштабну війну, тліючий військовий конфлікт на сході сприймався як те, що мало б колись закінчитися, контррозвідувальному забезпеченню Держприкордонслужби не надавалась належна увага.

Модель діяльності контррозвідки Держприкордонслужби функціонує в межах «Моделі правоохоронних органів», яка випливає з юридичних ознак або публічного права та базується на них. «Модель правоохоронних органів» передбачає більш стабільне робоче середовище «верховенства права». «Правоохоронна модель» також передбачає стабільну правову базу та реагує на злочинні дії відповідно до закону і піддається постійному судовому нагляду [4].

Означена модель діяльності контррозвідувальних органів піддається критиці. Так, колишній офіцер ЦРУ А. Хальнік зазначає, що мотиви та ресурси, які спонукають кримінальних злочинців до протиправної діяльності відрізняються від тих, які підтримуються іноземними розвідувальними службами. А тому навички кримінального розслідування дуже часто погано працюють у контррозвідувальних операціях [5]. С. Бекер у своїй праці намагався знайти відповідь на питання, чи повинні розвідники бути поліцейськими [6, с. 36]. Зазначений автор не дає чіткої відповіді на своє питання, проте, аргументуючи переваги та недоліки, звертається до думки практичних працівників розвідувальних органів, які зазначають: «проблеми поєднання поліцейської і розвідувальної моделі певною мірою виникатимуть незалежно від того, що ми робимо; ми не може-

мо повернутися до тих днів, коли розвідка та правоохоронні органи були відгороджені одне від одного; належна координація та добра воля з усіх сторін можуть мінімізувати шкоду» [6, с. 47].

У демократичних суспільствах усі служби змушені стикатися з проблемою досягнення балансу між секретністю та відкритістю. Підтримання рівня прозорості діяльності розвідувальних служб є найкращим способом забезпечення демократичної підзвітності та контролю, необхідних для підвищення обізнаності громадськості та підтримки розвідувальних служб. Однак потрібно бути завжди пильним: природа цієї діяльності така, що баланс між секретністю та демократією завжди буде делікатним [7].

Важливою проблемою «правоохоронної моделі» контррозвідувального забезпечення залишається недосконаліть оперативно-розшукового законодавства та його співвідношення з контррозвідувальною діяльністю в частині ведення, наприклад, оперативно-розшукових справ, негласних (слідчих) розшукових дій [8], а також відсутність у Держприкордонслужби права самостійно здійснювати досудове розслідування.

На цю проблему звертає увагу і С. Невмержицький зазначаючи, що чинні положення Кримінального процесуального кодексу України зневілювали саму суть проведення оперативно-розшукових і контррозвідувальних заходів, підмінивши їх негласними слідчими (розшуковими) діями, що не відповідають духу оперативності, актуальності, своєчасності, упереджувальності, прогнозованості, звужуючи оперативні й контррозвідувальні заходи та терміни їх виконання, а також, на жаль, прийняття лише тих даних як речових доказів, які були отримані саме в рамках кримінального провадження [9].

Але, очевидно, це така ціна функціонування демократичного суспільства, коли ефективний контроль за процедурами контррозвідувальної діяльності створює систему стримувань і противаг стримуючи до перетворення контррозвідувальних органів у репресивні структури.

Отже, незважаючи на існуючі недоліки у функціонуванні «правоохоронної моделі» контррозвідувального забезпечення Держприкордонслужби, вона відповідає демократичним, європейським устремлінням України і на сучасному етапі трансформації є більш правильною, оскільки її засадничий аспект – дотримання верховенства права.

Повномасштабне вторгнення рф в Україну загострило проблеми контррозвідувального забезпечення Держприкордонслужби і відкрило слабкі місця. Серед них можна відзначити такі:

– велике навантаження на оперативний склад підрозділів ВВБ Держприкордонслужби України;
– збереження державних секретів та забезпечення безпеки секретоносіїв;
– недоліки правового регулювання контррозвідувального режиму, що негативно позначається на якості та конкретності виконуваних завдань. Належна правова регламентація діяльності суб'єктів контррозвідувальної діяльності є важливою гарантією законності та дотримання прав і свобод людини і громадянина.

Варто також визнати, що однією із проблем контррозвідувального забезпечення є відсутність належної уваги до цієї дисципліни з боку науковців. Поодинокі наукові дослідження, присвячені цій темі, не спроможні наситити практику необхідними теоретичними знаннями. Потребує також активізація вивчення проблем контррозвідувального забезпечення і на рівні навчальних дисциплін. На жаль, цей перелік можна продовжувати, проте в межах відкритої публікації ми вимушені обмежитися лише деякими.

Отже контррозвідувальне забезпечення Держприкордонслужби містить систему окремих оперативно-розшукових, контррозвідувальних, режимних та адміністративно-правових заходів, що здійснюються гласно і негласно в інтересах забезпечення охорони та захисту державного кордону України, а також забезпечення безпеки своїх сил і засобів, інформаційних систем та оперативних обліків, запобігання загрозам, виявлення та припинення протиправної діяльності осіб або груп осіб, які створюють загрозу безпеці державного кордону України.

Одним з основних напрямів покращання контррозвідувального забезпечення Держприкордонслужби є удосконалення нормативно-правової основи її здійснення як на законодавчому, так і відомчому рівнях, підняття на новий рівень наукових досліджень у цій сфері, а також

збільшення штатної чисельності особового складу відділів контррозвідувального забезпечення Держприкордонслужби.

Потребує вивчення питання формування навчально-професійних програм за напрямком підготовки офіцерів ВВБ, яких планують призначати або вже призначили на посади офіцерів контррозвідувального забезпечення.

Список використаних джерел:

1. Про Державну прикордонну службу України: Закон України від 3 квітня 2003 року № 661-IV. Відомості Верховної Ради України (ВВР). 2003. № 27. ст. 208.

2. Про контррозвідувальну діяльність: Закон України від 26 грудня 2002 року № 374-IV. Відомості Верховної Ради України (ВВР). 2003. № 12. ст. 89.

3. Putter B. and Dov Bachmann S.– D. (2022): Scoping the Future Counterintelligence Focus. International Journal of Intelligence and CounterIntelligence, 1–28, 2022. doi.org/10.1080/08850607.2022.2091414

4. Britovšek J. Comparing Counterintelligence and Counterterrorism – Similarities, Issues and Solutions. VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 20 no. 2 P. 163–181.

5. Hulnick, Arthur S. Fall 1997. Intelligence and Law Enforcement: The ëSpies Are Not Copsí Problem. International Journal of Intelligence and Counterintelligence. Vol. 10, no. 3; P. 269–286.

6. Baker, Stewart L. Winter 1994/1995. Should Spies be Cops? Foreign Policy. No. 97; P. 36–52.

7. Intelligence PracticE and Democratic OversighT – A Practitioner's view. Dcaf Intelligence Working Group Geneva, July 2003. C. 74–75. URL: http://surl.li/onirj.

8. Половніков В.В., Халимон С.І. Проблеми правового регулювання оперативно-розшукової діяльності: пошук шляхів вирішення. Вісник Національної академії Державної прикордонної служби України. Серія: Юридичні науки. 2017. Вип. 3. URL: http://surl.li/qfgbf.

9. Невмержицький С. Проблеми правового впровадження контррозвідувальних та оперативно-розшукових матеріалів Служби безпеки України в контексті забезпечення національної забезпечення національної безпеки з протидії організованій злочинності. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану: тези Міжнародної науково-практичної конференції (Хмельницький, 24 листопада 2022 року). Хмельницький: Вид-во НАДПСУ, 2023 С. 694–695.

СТРАТЕГІЧНІ НАПРЯМИ ПОСИЛЕННЯ БЕЗПЕКОВОГО СЕРЕДОВИЩА УКРАЇНИ

Владислав ШЕНДРИК
доктор юридичних наук, професор,
заслужений юрист України
Національний юридичний
університет імені Ярослава Мудрого

Стратегічний аналіз безпекового середовища покликаний визначити процеси, явища, чинники, умови, обставини, події, результати діяльності й взаємодії суб'єктів суспільних відносин, а також тенденції їх розвитку, які впливають на рівень захищеності держави, суспільства, довкілля на певній території від наявних і прогнозованих загроз. Зміни безпекового середовища, що є відхиленням від його звичайного стану рівноваги, містять ризики, які підлягають подальшому аналізу. За результатами первинного аналізу безпекового середовища виявлені ризики можна розподілити на ті, що можуть трансформуватися в загрози, й ті, що створюють нові можливості для розвитку держави та суспільства [1, с. 23].

Трактуючи загрозу як потенційну причину небажаного інциденту, який може зашкодити фізичним особам, активам, системі або організації, навколишньому середовищу або суспільству, акцентуємо, що загрозу національній безпеці можуть створювати певні дії, явища, процеси, події, ситуації, безпосередньо спрямовані на підрив державного суверенітету і територіальної цілісності держави та/або здатні завдати шкоди життю, здоров'ю, майну громадян, завадити безперебійному наданню критично важливих функцій держави, завдати фізичної або економічної шкоди підприємствам, організаціям, об'єктам критичної інфраструктури, стати на заваді реалізації національних інтересів тощо. При цьому джерелом такої загрози може бути політика окремої держави або групи держав; окремі особи, групи людей, організації; природне середовище, зміни в діяльності, реалізації, функціонуванні або існуванні яких спричиняють ті чи інші загрози та визначають їхній загальний характер. З одного джерела може надходити більше ніж одна загроза [2, с. 19].

Серед інших джерел ризиків і загроз для національної безпеки України можна визначити такі: екологічні та техногенні загрози, розвиток науки і технологій, просування іншими державами інтересів, які суперечать національним інтересам України, тощо. Зазначені джерела ризиків і загроз є типовими для більшості держав, усунути їх повністю неможливо [3, с. 34].

На сучасне безпекове середовище відповідний вплив мають й глобалізаційні процеси, що відбуваються, а також вагома роль відводиться різноманітним загрозам, а надзвичайно важливі та актуальні постають ті, що пов'язані з розв'язаною війною проти України.

Отже, під час формування державної політики у сфері забезпечення національної безпеки держави мають застосовуватись інструменти, які дозволятимуть адаптуватися до постійної дії таких загроз. Такий підхід передбачає посилення національної стійкості держави.

Національна стратегія державної політики у сфері національної безпеки ґрунтується на трьох основних засадах:

– стримування – розвиток оборонних і безпекових спроможностей для унеможливлення збройної агресії проти України;
– стійкість – здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема, шляхом мінімізації зовнішніх і внутрішніх уразливостей;
– взаємодія – розвиток стратегічних відносин із ключовими іноземними партнерами, насамперед з Європейським Союзом і НАТО та їхніми державами-членами, США, прагматичне співробітництво з іншими державами та міжнародними організаціями на основі національних інтересів України [4].

Загалом своєчасне виявлення наявних і прогнозованих загроз національній безпеці, уразливостей і переваг (сильних сторін) держави і суспільства, а також можливостей посилення захисту національних інтересів в умовах певної безпекової ситуації, зважаючи на тенденції розвитку безпекового середовища, є підґрунтям для визначення стратегічних цілей і пріоритетів державної політики у сфері забезпечення національної безпеки. Основним методом проведення стратегічного аналізу безпекового середовища держави є SWOT-аналіз. Поглиблений аналіз ризиків і загроз національній безпеці передбачає також застосування низки кількісних і якісних методів дослідження [5].

Крім аналізу ризиків і загроз національній безпеці, стратегічний аналіз безпекового середовища передбачає також визначення вразливостей, переваг і можливостей держави та суспільства у сфері захисту національних інтересів.

Сучасне безпекове середовище характеризується високим ступенем мінливості й непередбачуваності. Часи, коли мир, криза і конфлікт були трьома чіткими фазами, коли під час конфліктів застосовувались в основному військові засоби, і коли супротивники були добре відомі, відійшли у минуле. Кібератаки завдають по країнах ударів нижче порогового рівня військового нападу. Кампанії в соціальних мережах створюють альтернативні реальності, спрямовані на дестабілізацію політичних громад, при цьому жоден солдат не перетинає жодного кордону. І «гібридна» комбінація військових і невійськових інструментів створює двозначні ситуації, які набагато ускладнюють ознайомлення з обстановкою і, відповідно, швидке прийняття рішень [6].

Важливо враховувати також можливість використання військових (у тому числі сепаратистських, ЧВК та інших сил) чи терористичних елементів у гібридних сценаріях. Всі ці аспекти потребують виважених стратегій відповіді, включаючи кіберзахист, підвищення інформаційної грамотності, міжнародного співробітництва та ефективних політичних рішень для забезпечення національної безпеки та стабільності.

Україна зустрічається з різноманітним спектром гібридних атак, які становлять серйозний виклик для її безпеки та стабільності. Інформаційна війна виявляється через масштабну дезінформацію та пропаганду, спрямовану на вплив на громадську думку та події в країні. Кібератаки на критичну інфраструктуру, фінансові установи та державні системи стають все більшим викликом, загрожуючи як звичайним господарським процесам, так і національній безпеці. Економічний тиск, включаючи санкції та торгові обмеження, спрямований на послаблення економіки, є ще однією складовою гібридних загроз. Політичні маніпуляції та втручання в політичні процеси можуть призводити до дестабілізації влади та впливу на прийняття стратегічних політичних рішень. Енергетичний тиск, включаючи атаки на енергетичну інфраструктуру, може створювати серйозні виклики для забезпечення енергетичної незалежності та безпеки країни.

Невизначеність ситуацій пов'язаних із застосуванням «гібридних атак» суттєво ускладнюють формування державами політики у сфері національної безпеки, потребує диверсифікації заходів, посилення традиційних безпекових механізмів заходами у сфері побудови національної стійкості. Наведене вище актуалізує пошук нових, теоретично обґрунтованих підходів до забезпечення національної безпеки, у тому числі стратегічного аналізу і планування.

Ключові орієнтири держави у сфері забезпечення національної безпеки полягають в тому, що Україна повинна сформувати достатні власні спроможності як фундаментальну основу щодо забезпечення своєї безпеки й створення системи цілісного стратегічного аналізу воєнних загроз національній безпеці Української держави, розвиток об'єднаних розвідувальних спроможностей сил оборони з ціллю отримання повної і достовірної інформації щодо своєчасного прийняття рішень з приводу забезпечення воєнної безпеки країни; гарантування спроможності держави швидко пристосовуватися до змін безпекового середовища, оперативно й ефективно протистояти воєнним загрозам, безперебійно функціонувати до та в період воєнного конфлікту, а також в короткі терміни відновлюватися після його завершення [7, с. 55].

За умов мінливості безпекового середовища особливого значення набуває впровадження адаптивного управління у сфері забезпечення національної безпеки. Передусім це передбачає здійснення в державі регулярного аналізу безпекового середовища з метою своєчасного внесення коректив до цілей і завдань державної політики відповідного спрямування.

Ґрунтуючись на вищевикладеному можна виокремити аспекти забезпечення безпекового середовища в умовах гібридних загроз як складової національної безпеки, а саме:

- розробка стратегічних операційних процедур і планів реагування на кризові ситуації із визначенням сценаріїв та повноважень суб'єктів державного управління;
- створення моделей (стратегічне моделювання) та їх практичне відпрацювання під час тренувань;
- ідентифікація викликів і загроз, стратегічне прогнозування їх проявів та розробка сценаріїв реагування на них;
- адекватне реагування на кризові ситуацій в розрізі інформаційної безпеки із застосуванням технологій, спрямованих на нівелювання інформаційних атак;
- налагодження кризових комунікацій у докризовий період для поширення верифікованої інформації із державним і приватним секторами;
- аналіз ризиків та розробка стратегій запобігання і реагування на кризові ситуації із врахуванням потенційно можливих нових загроз, відповідь на комплексні, довготривалі, змішані гібридні атаки;
- моніторинг обстановки та оцінка заходів забезпечення безпекового середовища, а також коригування стратегій у разі появи нових загроз і викликів.

Список використаних джерел:

1. Резнікова О.О. Стратегічний аналіз безпекового середовища України. Стратегічні пріоритети. 2022. № 9. С. 22–28.
2. Резнікова, О. О. (2022). Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 456 с.
3. Криворучко, І., Щур, Н., Семенець-Орлова, І. (2024). Концептуальні засади розвитку безпекового середовища в Україні. Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління, (6 (72)), 33–43. URL: https://doi.org/10.32689/2523–4625–2023–6(72)-5. (дата звернення: 12.06.2024)
4. Президент України (2020). Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. Президент України Володимир Зеленський: офіц. інтернет-представництво. URL: https://www.president.gov.ua/documents/3922020–35037. (дата звернення: 12.06.2024)
5. Резнікова, О. О., Войтовський, К. Є., Лепіхов, А. В. (2020). Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України: аналіт. доповідь / за заг. ред. О.О. Резнікової. Київ: НІСД, 84.
6. Michael Rühle, Clare Roberts (2021). Enlarging NATO's toolbox to counter hybrid threats, 19 March. URL: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybridthreats/index.html. (дата звернення: 12.06.2024)
7. Глущенко О.О. Функція забезпечення безпеки держави в умовах воєнного стану. Часопис Київського університету права. № 1. 2023. С. 53–56.

ЩОДО УДОСКОНАЛЕННЯ СИСТЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНОГО ОБСЛУГОВУВАННЯ КРИМІНАЛЬНОЮ ПОЛІЦІЄЮ ЛІНІЇ РОБОТИ ЩОДО НЕЗАКОННОГО ЗАВОЛОДІННЯ ТРАНСПОРТНИМИ ЗАСОБАМИ

Олександр ЯКОВЧЕНКО
аспірант
Дніпровського державного
університету внутрішніх справ

Стрімка інтеграція та уніфікація управлінських процесів у правоохоронній сфері, достатньо високий рівень злочинності в Україні вимагають постійного розвитку Національної поліції України як центрального органу виконавчої влади та застосування нових концептуальних підходів до організаційно-правового забезпечення її діяльності. Від результативності роботи Національної поліції України залежить публічна безпека і порядок, захист прав та інтересів людини. Тому метою удосконалення поліції є поетапне створення правоохоронного відомства світового зразка, в якому будуть оптимізовані системи управління та прийняття рішень, а завдання виконуватимуться ефективно [1].

Процеси становлення та розвитку правової держави неможливі без формування і розробки дієвих правових важелів впливу на суспільно небезпечні явища, які тягнуть за собою настання юридичних наслідків [2].

Одним із дієвих способів досягнення такої мети є удосконалення нормативно-правового забезпечення діяльності як Національної поліції України у цілому так і її підрозділів зокрема.

З огляду на це актуальним є вироблення та надання пропозицій щодо вдосконалення правового забезпечення оперативного обслуговування кримінальною поліцією лінії роботи щодо незаконного заволодіння транспортними засобами.

За статистичними даними, рівень злочинності, пов'язаної з незаконним заволодінням транспортними засобами, за останні 5 років упав втричі/ Водночас рівень оголошених підозр по вказаних кримінальних провадженнях залишається досить низьким (приблизно 2200 підозр в рік). Тобто у більше ніж половині випадків не було встановлено особу злочинця. Така ситуація зумовлена багатьма факторами, серед яких й низький рівень оперативного обслуговування кримінальною поліцією лінії роботи щодо незаконного заволодіння транспортними засобами [3].

Незважаючи на значний інтерес вчених до проблем протидії незаконного заволодіння транспортними засобами на сьогодні у правовому регулюванні вказаної діяльності залишається значна кількість невирішених проблем.

З метою виявлення наявних прогалин, а також визначення шляхів удосконалення системи **правового забезпечення** оперативного обслуговування кримінальною поліцією лінії роботи щодо незаконного заволодіння транспортними засобами нами було здійснено порівняльний аналіз наукових доробок авторів з діючими на сьогодні нормативними актами на предмет нормативного забезпечення проблемних питань на яких автори робили акцент. Проведений аналіз показав, що значна кількість визначених авторами пропозицій не була врахована або не відповідає сучасному нормативному забезпеченню. Враховуючи зазначене пропонуємо внесення змін до окремих нормативно-правових актів, зокрема:

1) графу «викрадені транспортні засоби, які розшукуються у зв'язку з безвісним зникненням особи, виявлені безгосподарні транспортні засоби, а також викрадені, втрачені номерні знаки» додатку до постанови Кабінету Міністрів України від 14.11.2018 № 1024 «Про єдину інформаційну систему Міністерства внутрішніх справ» викласти у такій редакції: «транспортні засоби, які розшукуються, у тому числі у зв'язку з безвісним зникненням особи, виявлені безхазяйні транспортні засоби, а також викрадені, втрачені номерні знаки»;

2) абз. 4 п. 25 розділу XX Інструкції про організацію оперативно-розшукової діяльності та негласної роботи оперативними підрозділами Національної поліції України, затвердженої наказом МВС України від 05.05.2016 № 07 викласти у такій редакції: «4)»Угон» – база даних, у якій обліковуються відомості про транспортні засоби (автомобілі, мотоцикли, мопеди, плавзасоби тощо), які розшукуються органами (підрозділами) Національної поліції України, правоохоронними органами інших держав;»;

3) доповнити пункт 3 розділу IV Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, затвердженої наказом МВС України від 07.07.2017 № 575 абзацом наступного змісту: «Працівники оперативних підрозділів кримінальної поліції залучаються до складу слідчо-оперативної групи залежно із врахуванням їхньої спеціалізації за лініями роботи (видом кримінальних правопорушень, на протидії яким вони спеціалізуються).».

Список використаних джерел:

1. Авагімов А.А. Оперативно-розшукова протидія незаконному заволодінням транспортними засобами, поєднаному з насильством, небезпечним для життя чи здоров'я потерпілого: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.09. Харків: ХНУВС, 2021. 20 с.

2. Кудінов С.С. Шляхи удосконалення правового регулювання забезпечення Службою безпеки України антитерористичної безпеки. Підприємництво, господарство і право. 2019. № 2. URL: http://pgp-journal.kiev.ua/archive/2019/2/45.pdf. (дата звернення: 18.06.2024)

3. Дараган В.В., Яковченко О.І. Визначення основних напрямів дослідження проблемних питань організації оперативного обслуговування кримінальною поліцією лінії роботи щодо незаконного заволодіння транспортними засобами. Науковий вісник Дніпропетровського державного університету внутрішніх справ: Науковий журнал. 2022. № 1 (116). С. 229–233.

Секція 3
ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ СБУ З РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З РОЗПОВСЮДЖЕННЯМ ТА ЗАСТОСУВАННЯМ РАДІАЦІЙНОЇ, ХІМІЧНОЇ, БІОЛОГІЧНОЇ ТА ЯДЕРНОЇ ЗБРОЇ

PREVENTION OF CHLORINE LEAKAGE BY DEPOSITION IN THE CONDITIONS OF MILITARY AGGRESSION

Andrii LESKO
Post-graduate student of National University
of Civil Protection of Ukraine (city Kharkiv)
Oleg KULAKOV
Ph.D (Technical sciences), Associate Professor,
Senior Researcher of Scientific Department of Problems
of Civil Protection and Technogenic and Ecological Safety
of the Scientific and Research Center of National University
of Civil Protection of Ukraine (city Kharkiv)

From a military point of view, chlorine is a chemical warfare agent and is also used in the production of chemical warfare agents, such as mustard gas and phosgene. As a chemical warfare agent, chlorine was first used during World War I on April 22, 1915, near the city of Ypres (Belgium). German army released about 180 tons of chlorine on the positions of British and French arms. About 15,000 people were injured, of whom about 5,000 died. On July 13, 1917, mustard gas was used as a chemical weapon near that city [1].

Chlorine is also widely used in civilian industry and everyday life.Chlorine is used for industrial disinfection of drinking water, as a raw material for the production of polyvinyl chloride and plastics, and is used in the production of insecticides for pest control in agriculture, etc.

The widely civilian use of chlorine leads to relatively frequent accidents with its release. In Ukraine, the latest known chlorine leakage accident occurred on December 1, 2021, at a facility in Odesa. The 800-liter tank was destroyed. To localize the accident, water was supplied in spray streams [2].

On February 28, 2019, a chlorine leak occurred at the Birmingham Water Works in Alabama (USA). More than 50 people were hospitalized [3]. Birmingham Water Works believes that the leak was caused by a violation of the production process at the enterprise.

On February 24, 2022, the Russian Federation began an open military attack on Ukraine. The risk of accidents involving the release of the hazardous chemical chlorine has increased significantly. There is a threat of both accidental and direct destruction of industrial chlorine tanks by the enemy.

Chlorine is a pale yellow-green gas with a characteristic odor (odor perception occurs at a concentration of 0.3÷3.8 mg/m3, the maximum permissible concentration is 5 mg/m3). Chlorine gas is 2.5 times heavier than air, so it tends to accumulate in low areas, basements, etc.

Chlorine liquefies at a temperature of minus 34 °C. Evaporating in the air. Liquid chlorine forms a white mist with water vapor. Chlorine in the cloud is in lethal concentrations. Chlorine is a strong

oxidizing agent. Wet chlorine causes severe corrosion of most metals. The presence of chlorine in the air causes internal combustion engines to stall and damage them [4, 5].

Chlorine is a potent toxic substance that has a general toxic and irritating effect on the human body and causes chemical burns. The first signs of exposure are sharp chest pain, impaired coordination, stinging eyes, mucous flow, dry cough, and vomiting. Chlorine causes severe irritation of the mucous membranes of the eyes, upper and deep respiratory tract and lungs.

In point of view of fire hazard, it is a non-flammable substance. It is an oxidizing agent. Many metals and non-metals (titanium, copper, aluminum, zinc, phosphorus, etc.) can burn in the atmosphere of dry and moist chlorine gas.

Chlorine is stored in special tanks or pumped into high-pressure steel cylinders. Pressurized liquid chlorine cylinders have a special coloring – a protective color with a green line. During long-term operation of chlorine tanks, extremely explosive nitrogen trichloride accumulates in them, and therefore, from time to time, chlorine tanks must periodically washing and cleaning from nitrogen chloride.

Chlorine dissolves in water to form hydrochloric acid HCl and hypochlorous acid HClO:

In terms of its chemical activity, hydrochloric acid HCl is one of the strongest acids. The properties of hydrochloric acid depend significantly on its concentration in aqueous solution. Concentrated hydrochloric acid contains 37% HCl and has a density of 1.19 g/cm³. Hydrochloric acid is present in a concentration of about 0.5% in the human stomach.

Hypochlorous acid HClO is a weak acid in terms of its chemical activity. It is used as a disinfectant.

At 10 °C and atmospheric pressure, one liter of water dissolves 3.10 liters of gaseous chlorine, while at 30 °C, 1 liter of water dissolves only 1.77 liters of chlorine. As the pH of the solution increases (with increasing alkalinity), the solubility of chlorine in water increases.

The issue of predicting the consequences of chlorine releases during accidents, organizing firefighting and emergency response to chlorine-related accidents, and protecting personnel of the civil protection rescue service has been relevant since Ukraine gained independence. Today, the main departmental documents in force on this issue are the following orders [6–8].

Extinguish a fire in the presence of chlorine with water from the greatest possible distance. Cool containers with water. Use spray water to disperse (settle, isolate) vapors. The hazardous area is located within a radius of at least 200 meters. The size of the chemical contamination zone is specified based on the results of chemical reconnaissance. The hazardous area must be entered only in personal protective equipment. Keep to the windward side and avoid low places. Do not contact the substance that has been spilled. Provide first medical aid to the victims. Involve services in accordance with the accident localization and response plan to eliminate leaks, pump it into a serviceable container, enclose spill sites with an earthen berm, and neutralize spills. Remove combustible materials from the accident area. Do not allow it to enter water bodies, basements, or sanitary sewers.

Insulating thermal and gas protective suit (for example, ІК-ТГЗ), insulating gas and chemical protective suits (for example «Рятувальник 2МУ» or «Рятувальник 3У») should be used as personal skin protection equipment. Personal respiratory protection equipment – any insulating protective breathing apparatus.

To protect the human body, it is possible to use not only specialized personal protective equipment, but also conventional equipment adopted by the Armed Forces of Ukraine. To protect the human body, it is possible to use a general military protective kit ZZK. To protect the respiratory system, military gas masks with special filters (e.g., B1P1D chlorine, the protective effect time does not exceed 20 minutes) can be used.

In the conditions of military operations, the liquidation of the consequences of the chlorine accident is complicated by the possibility of additional combat damage to the personnel of the civil defense operational and rescue service, the military and the civilian population.

List of used sources:

1. Ypres. Belgium. URL: https://en.wikipedia.org/wiki/Ypres (reference date 18.06.2024).
2. В Одесі стався витік хлору. URL: https://podrobnosti.ua/2429768-v-odes-stavsja-vitk-hloru.html (reference date 18.06.2024).
3. На водоочисній станції у США стався витік хімікатів, госпіталізовано півсотні людей. URL: https://blitz.if.ua/index.php/news/na-vodoochysniy-stancii-u-ssha-stavsya-vytik-himikativ-gospitalizovano-pivsotni-lyudey.html (reference date 18.06.2024).
4. Chlorine. URL: https://en.wikipedia.org/wiki/Chlorine (reference date 17.05.2024).
5. SFPE (Society of Fire Protection Engineers) Handbook of Fire Protection Engineering: 5th edition / Morgan J. Hurley. Quincy: National Fire Protection Association, 2016. 3493 p.
6. Рекомендації щодо організації гасіння пожеж підрозділами МНС на промислових об'єктах підвищеної небезпеки з наявністю небезпечних хімічних речовин: Наказом МНС України від 29.09.2011 р. № 1017. URL: https://ips.ligazakon.net/document/FIN69119 (reference date 18.06.2024).
7. Статут дій органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту під час гасіння пожеж: Наказ МВС України від 26.04.2018 № 340. URL: https://zakon.rada.gov.ua/laws/show/z0801–18#Text (reference date 18.06.2024).
8. Методика прогнозування наслідків виливу (викиду) небезпечних хімічних речовин під час аварій на хімічно небезпечних об'єктах і транспорті: Наказ МВС від 29.11.2019 р. № 1000. URL: https://zakononline.com.ua/documents/show/485712___653617#n13 (reference date 18.06.2024).

ЩОДО НЕОБХІДНОСТІ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ НА ТЕМУ ХІМІЧНОЇ, БІОЛОГІЧНОЇ, РАДІОАКТИВНОЇ ТА ЯДЕРНОЇ (РХБЯ) ЗАГРОЗИ ТА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД ЗБРОЇ МАСОВОГО УРАЖЕННЯ

Костянтин АБРАМОВ
старший викладач Національного юридичного
університету імені Ярослава Мудрого
Микола КОРЧАГІН
кандидат наук з фізичного виховання і спорту, доцент,
завідувач кафедри Національного юридичного
університету імені Ярослава Мудрого

Після початку військової агресії РФ проти України в березні 2014 р., анексії Криму та повномасштабного вторгнення 24 лютого 2022 року виникли серйозні проблеми, пов'язані з можливими диверсійними актами, направленими на ослаблення нашої держави. Одним із видів найнебезпечніших диверсійних проявів може бути застосування деяких видів зброї масового ураження, а саме – тероризм, пов'язаний із використанням ядерної зброї, руйнуванням об'єктів атомної енергетики та промисловості, хімічний та біологічний тероризм.

Стосовно можливих ядерних загроз війни.

Володимир Зеленський 22 червня минулого року заявив, що за даними розвідки, росія розглядає сценарій «терористичного акту» з викидом радіації на Запорізькій АЕС. Про загрози на захопленій атомній станції посадовці та експерти говорять постійно, у той час як імовірність використання Росією тактичної ядерної зброї називають малоймовірною чи й взагалі неможливою.

Вже другий рік путін та інші посадові особи Росії вдаються до ядерних погроз. Найгучніше вони пролунали на початку осені 2022 року, спричинивши жорстку реакцію інших ядерних держав. Тоді, путін попередив, що у разі загрози «територіальній цілісності» Росія використає «всі наявні засоби, і це не блеф», маючи на увазі тактичну ядерну зброю.

У лютому 2023 року розвідка Норвегії повідомила, що кораблі російського військово-морського флоту почали виходити в море з тактичною ядерною зброєю – вперше за останні 30 років. Згідно з дослідженням, основну частину ядерних сил розмістили на підводних човнах і кораблях Північного флоту. Наступним кроком путіна стало розміщення тактичної ядерної зброї на території Білорусі.

Нещодавно рашиський президент знову заявив, що використання ядерної зброї вважає «теоретично можливим». Підстави – ті ж самі, про які він казав раніше: якщо буде загроза територіальній цілісності, незалежності і суверенітету Росії. Зараз, наголосив Путін, «немає такої потреби». Він також заявив, що Росія має більше ядерних озброєнь, ніж країни НАТО.

Утім, шлях до застосування тактичної ядерної зброї – не короткий. Ця зброя, на відміну від стратегічної, зберігається далеко від місць, звідки її можуть застосувати. Згідно з неофіційними даними, Росія зберігає ядерну зброю в основному на території Сибіру. Доставка її у спеціальних ешелонах навряд чи може відбутися непоміченою.

Окремо увагу потрібно приділити питанню збільшення незаконного обороту ядерних матеріалів, джерелами яких можуть бути об'єкти атомної енергетики, промисловості, науково-дослідницькі заклади на тимчасово окупованих територіях України. Кінцевий ризик в тому, що представники держави-ізгоя або добре організована терористична група можуть придбати достатню кількість ядерних матеріалів та використати з терористичною метою: виробити саморобний ядерний пристрій (Аль-Каїда, 2002 рік), радіологічний розсіювальний пристрій або «брудна бомба», здійснити отруєння (2006 рік – Олександр Литвиненко отруєний Ро-210, вжитим з продуктами харчування), використати у формі аерозолю (розсіювання з БПЛА), виробити пристрій радіологічного опромінення (із прихованим розміщенням в місцях з постійною великою кількістю людей) та інші.

Наш ворог жорстокий, безпринципний та божевільний. Ніхто не може гарантувати на 100%, що росіяни все ж не наважаться використати свій ядерний арсенал, і що загрози так і залишаться загрозами. Тому ми, українці маємо бути готові до всього, вміти фільтрувати та аналізувати інформацію, отриману з різних джерел, аби уникнути зайвої паніки та не піддаватися на ворожу пропаганду.

Хімічна зброя та біологічний тероризм. Як свідчать останні події триваючої жахливої війни в державі, загроза застосування зброї масового знищення, включаючи хімічну зброю, з боку росії проти України постійно нависає. Ми всі дуже сподіваємося, що такий жахливий сценарій розвитку подій ніколи не станеться в реальному житті. Проте зважаючи на те, що війна триває, а сусідня країна-терорист, хоч і є однією зі 193 країн, які зобов'язалися «ніколи, за жодних обставин не розробляти, виробляти, купувати, накопичувати, передавати або використовувати хімічну зброю» проти інших країн, постійно порушує цю угоду та не дотримується законів та правил ведення війни. І це обумовлює важливість висвітлення цієї тематики. Росія може застосувати в Україні хімічну або біологічну зброю. Про це неодноразово попереджали США та інші наші партнери. Передувала цьому чергова брехня кремля про наявність в Україні «таємних біологічних лабораторій», що дуже схоже на провокацію, аби можна було в усіх гріхах звинуватити нашу державу.

Будь-яке використання зброї росією буде порушенням міжнародного права, Конвенції щодо заборони хімічної зброї, що підписана самою країною-окупантом. Втім, як показує життя, від східного сусіда-агресора можна очікувати чого завгодно.

Інформаційні вкроси на високому рівні – з боку військового керівництва фашистської росії – говорять про те, що плани використання хімічної зброї є. Такі типи зброї можуть використовуватися як для провокацій, так і для поразки цивільного населення. Це вписується і в офіційну ідеологічну риторику кремля щодо «остаточного розв'язання українського питання», «деукраїнізації України», що практично стовідсотково збігається з риторикою третього рейху з «остаточного розв'язання єврейського питання».

Зброя масового ураження буває трьох типів: ядерна, хімічна і біологічна. Наші міжнародні партнери, керівництво НАТО більше уваги приділяють можливості застосування росією ядерної зброї. А я вважаю, що використання хімічної зброї на сучасних ракетних носіях становить дуже серйозну загрозу насамперед для цивільного населення, тому що в нас досить велика щільність населення. Саме така небезпека має розглядатися нами та нашими партнерами насамперед. Тож, сценарій застосування хімічної зброї в Україні вважаю цілком реальним.

Окреме місце потрібно відвести біологічному тероризму, а саме використано біологічних засобів ведення війни (бактерій, вірусів, рикетсій, грибків, токсинів або речовин, вироблених цими організмами) проти населення та військ з метою загрози знищення або знищення максимальної кількості людей.

Історичні джерела засвідчують, що СРСР приєднався до конвенції про заборону розробки, випробування і виробництва біологічної зброї. Тоді ж, вперше, штучно був створений ген. І біологи в погонах направили в ЦІК КПРС лист: «Якщо генетику застосувати до воєнної мікробіології, вийде найпотужніша зброя, яка нашим вірогідним супротивникам і не снилася. І виріс ще один «чумний архіпелаг»: Інститут прикладної мікробіології в Оболенську (Серпухівський район, росія) зайнявся бактеріями; у потужний вірусологічний центр в Кольцові (30 км від Новосибірська, зараз називається «Вектор») перенесли роботи з воєнного використання натуральної віспи; в тодішньому Ленінграді створили Інститут «особливо чистих речовин»; у Степногорську (Казахстан) – дуже потужний Інститут мікробіології. У Ленінграді займалися білками, пептидами: вважалося, що з їх допомогою можна управляти психікою людини. Власне, це й було головною метою досліджень: добитися, щоб бактерії в процесі своєї життєдіяльності виділяли білок, який міг би впливати на мозок солдатів супротивника. З'явилися такі інститути і в москві: біологічного приладобудування і «Біомашпроект». Ще один НДІ виник біля Чехова. На заводі в Бердську Новосибірської області поставили на потік віруси з Кольцово. Крім цього спорудили ще мобілізаційні заводи в Кургані й Пензі, які й досі перебувають у мобілізаційній готовності. Є відомості про те, що у 70-ті рр. минулого століття радянські розвідники роздобули в Індії збудника натуральної віспи. Зброя на базі віспи випускалася в Загорську ще з 40-х рр., але індійська виявилася ефективнішою. Адже натуральна віспа це, по суті, війна проти всього світу: у 1980 р. ВООЗ повідомила про те, що досягнута планетарна елімінація вірусу натуральної віспи. У зв'язку з цим і щеплення проти цієї недуги були припинені. А це означає, країна, яка зберігає зазначеного збудника, володіє зброєю, до якої чутлива більшість людей на Землі. Примітно, що радянські спецслужби за будь-яку ціну намагалися роздобути смертоносні віруси геморагічних гарячок, болівійської, Ебола, Ласса, Марбурга.

Вказані підприємства та організації ще й досі працюють на території рф, що значно підвищує можливість застосування біологічної зброї російськими військами.

Порівняно з іншими видами озброєння (ядерне, хімічне, звичайне) біологічна зброя унікальна у своєму різноманітті.

Наявність реальної загрози раптового застосування противником біологічної зброї, як і поява у військах та серед цивільного населення масштабних спалахів та епідемій небезпечних інфекційних захворювань, здатні повсюдно викликати страх, панічний настрій, знижувати боєздатність військ, дезорганізовувати роботу тилу.

Поряд із безпосередніми РХБЯ загрозами у сучасному світі набирає актуальності проблема боротьби з дезінформацією про РХБЯ інциденти та загрози.

Дезінформація на тему хімічної, біологічної, радіоактивної та ядерної (РХБЯ) загрози може бути дуже шкідливою і мати жахливі наслідки. Ця її властивість стала ще більш актуальною сьогодні, коли інформація є легкодоступною й нерозважливо поширюється без перевірки її достовірності. Підроблена або шахрайська інформація про надзвичайні ситуації, пов'язані з РХБЯ чинниками, як-от терористичні атака або пандемії, може вводити в оману уряди та міжнародні організації, знецінювати заходи реагування, призводити до неправильного спрямування й марнування ресурсів та викликати паніку серед населення. Хибна інформація, до якої також належать теорії змови, може також підсилювати страх та тривогу серед цільових категорій

населення, якщо вона, наприклад, повідомляє, що подія, пов'язана з РХБЯ загрозою, вийшла з-під контролю. Вона навіть може спричинити суспільний хаос, якщо частина населення повірить, що подія, пов'язана з РХБЯ загрозою, була навмисно й свідомо організована та є частиною зловмисного плану. Хибна інформація може також використовуватися для радикалізації й втягнення несвідомих осіб у терористичну діяльність, оскільки вона може підсилювати страх й підігрівати ненависть серед різних категорій населення.

Отже, під час сучасних бойових дій не можна недооцінювати важливість ведення радіаційної, хімічної та біологічної (РХБ) розвідки та радіаційного хімічного спостереження, збору та обробки інформації про РХБ обстановку, а також проведення лабораторних аналізів води, продуктів харчування та вміння використання сучасних засобів індивідуального і колективного захисту, а також впевнене застосування засобів, що містяться в індивідуальних аптечках.

Враховуючи все вище вказане, слід вживати серйозних заходів не тільки щодо запобігання можливим диверсіям але й вміти аналізувати, розуміти дезінформацію на тему РХБЯ загрози в засобах масової інформації, на платформах соціальних мереж та ефективно реагувати на неї.

Список використаних джерел:

1. Posetti, J., & Matthews, A. (2018 p.). A short guide to the history of 'fake news' and disinformation: A new ICFJ learning module. Міжнародний центр для журналістів. (дата звернення: 18.06.2024)

2. UNICRI Посібник з боротьби з дезінформацією на тему РХБЯ загрози. Міжрегіональний науково-дослідницький інститут Організації Об'єднаних Націй з питань злочинності й правосуддя (ЮНІКРІ), грудень 2022 р. URL: https://issuu.com/unicri/docs/handbook_cbrn_disinformation_uk_.(дата звернення: 18.06.2024)

3. Ядерні загрози війни. Чого чекати від Росії. URL: https://www.bbc.com/ukrainian/articles/c6pl060jrz1o. (дата звернення: 18.06.2024)

4. Вторгнення Росії в Україну. 1–30 червня 2023 року. URL: https://ua.korrespondent.net/ukraine/politics/4603508-vtorhnennia-rosii-v-ukrainu-1–30-chervnia-2023-roku. (дата звернення: 18.06.2024).

RISK ANALYSIS IN THE CONTEXT OF CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR THREATS

Oleksandr HALAK
candidate of Technical Sciences, Associate Professor
Head of the Department of CBRN Protection
of the Faculty of CBRN Protection and
and Environmental Safety of the Military
Institute of Tank Troops of NTU 'KhPI'
Dmytro ANISHCHENKO
senior Lecturer at the Department of CBRN Defence
of the Faculty of CBRN Protection and
environmental safety of the Military
Institute of Tank Troops of NTU 'KhPI'

In today's world, where challenges and threats are becoming increasingly complex and international, risk analysis in the area of national security is becoming a vital task. This task takes on a special dimension in the context of chemical, biological, radiological and nuclear (CBRN) risks, which can have unpredictable and serious consequences for the nation's security. Effective national security risk management requires a thoughtful approach that analyses a wide range of aspects, from political and economic to social and technical.

Risk analysis in the context of chemical, biological, radiological and nuclear threats is a specialised field that aims to identify and assess the possible adverse effects of the characteristics of these types of threats. This methodology takes into account the high degree of uncertainty and potential complexity of such hazards, using advanced technologies and innovative approaches to reduce risks and maximise safety.

The result may be the abandonment of an operation or a significant change in the pace, timing and objectives of an operation.

CBRN defence units determine the vulnerability of the troops (forces) to CBRN threats, the value of which may affect their actions. Vulnerability of troops (forces) to CBRN threats is the level of possible losses of personnel caused by the impact of CBRN threats.

Vulnerability is a manifestation of the properties of the troops (forces) (engineering, technical, organisational, moral and psychological) in terms of their ability to withstand the relevant negative impact. The magnitude of vulnerability to CBRN threats depends on the following factors:

– shortcomings in planning an operation to deploy troops (forces) without taking into account the protective properties of the area and the close proximity to CBRN hazardous facilities;
– the level of training of troops (forces) to perform CBRN protection tasks;
– level of coordination of troops (forces) in terms of their mobility;
– imperfection of the system of detection and warning of CBRN threats and/or its insufficient coverage of the territory covering the area (district) of operation;
– lack of appropriate collective and individual protection means for the damage factors;
– failure to take into account meteorological (weather) conditions.

The risk assessment takes into account four factors and should include

Prioritisation of risks to support the decision-making process:

– the likelihood of an incident caused by a threat or hazard;
– the likelihood of exploitation of a specific vulnerability of the facility;
– the impact of losses on the success of the operation in terms of the number of fatalities or the number and severity of injuries to personnel;
– failure of (damage to) weapons and military equipment (facilities), loss or damage to information or other factors affecting the success of the operation.

In the case of a high CBRN risk, it is necessary to develop control measures and determine the most effective way to eliminate (neutralise) the CBRN risk according to the criterion that provides the best balance between availability and effectiveness. In this phase, measures to counter CBRN risks are continuously implemented, and measures that delineate the CBRN hazard are analysed and monitored to identify any residual risk.

Risks from weapons of mass destruction (hereinafter referred to as WMD) and chemical, biological, radiological and nuclear (hereinafter referred to as CBRN) include the threat of serious and widespread adverse effects on people, the environment and society as a whole.

Mass destruction could result from the use of nuclear weapons, chemicals, biological agents or radioactive materials by criminals or terrorists. These risks include the possibility of a large number of casualties, severe environmental impact, and long-term health and environmental consequences.

Preventive measures and international cooperation, including controlling the proliferation of WMD and CBRN weapons, are essential to reduce these risks and ensure global security and safety:

1. Chemical weapons.

Chemicals can cause serious and even fatal consequences for humans and animals. The spread of poisonous substances can lead to large-scale infections, and the threat can extend over large areas. 2. Біологічна зброя.

The use of pathogenic microorganisms or toxins can lead to the massive spread of diseases and epidemics. Impact on natural ecosystems and biodiversity.

3. Radiological weapons.

Radioactive materials can cause radiation damage to living organisms. The use of radioactive substances can lead to prolonged periods of environmental contamination.

4. Nuclear weapons.

Extensive destruction and loss of life as a result of a nuclear explosion. Widespread radiation effects and the possibility of a nuclear winter affecting the climate and ecosystems. The use of any of these weapons could have far-reaching consequences for humanity, the environment and geopolitical stability. Countering these threats requires international cooperation, proliferation control and effective security measures.

The implementation of nuclear weapons and nuclear terrorism includes various possible scenarios that could be carried out by states or terrorist groups.

Preventing nuclear terrorism requires international cooperation, enhanced oversight of nuclear materials and weapons, and the ability to monitor and prevent possible threats. This is a complex task that requires joint efforts from states and international organisations.

Maintaining sufficient dual-use capabilities to escalate to nuclear use is an ongoing concern for Russia, given NATO's ability to threaten these capabilities with conventional and, according to these authors, cyber weapons.

The discussion of the first use of nuclear weapons leads to a certain level of confusion for Western analysts. On the one hand, Russia continues to emphasise that it has no formal policy of 'escalation to de-escalation'. Russian military doctrine allows for the use of nuclear weapons in response to a conventional attack. This is not called 'escalation to de-escalation', but nuclear first use is present in Russian doctrine. U.S. planning is properly preparing for a situation in which Russia suffers conventional attacks and resorts to the use of nuclear weapons against a military objective.

In the context of the Russian military strategy, it is stated that Russia may use nuclear strikes in response to threats to its statehood, including the use of nuclear and other weapons of mass destruction against it. It is noted that such a situation could arise as a result of a fabricated pretext, such as accusing Ukraine of chemical or biological attacks, creating a potential threat of a limited or full-scale nuclear war against it and the United States and NATO in Europe.

In a similar context, there is debate about the possibility of destroying sensitive targets as an asymmetric means of overcoming NATO's superiority in a conflict with a non-compliant adversary such as Russia. A British parliamentary report highlighted the death of a Russian secret agent in London in 2006, calling the assassination an 'act of nuclear terrorism on the streets of a major city' that put the lives of civilians at risk.

Unlike Ukraine, our Western partners have something to respond to Russia. Today, the United States (both on its territory and in Europe), the United Kingdom and France have nuclear weapons, which is a powerful deterrent to Russia.

However, given the absolute inadequacy of the Kremlin leader, he may decide to start a nuclear war with the United States and NATO. Even in the most difficult times for the Russian Federation during the economic crisis of the 1990s, Moscow made every effort to maintain and improve its strategic nuclear potential. And since 2007, after the Kremlin's move to confrontation with the West, such measures have become much more extensive.

A new vision of the security and safety risk has been made possible by technological advances and changes in the geopolitical environment. This has resulted in the emergence of new types of threats and risks that require new approaches and methods for their assessment and risk management. However, using the risk analysis methodology, these risks can be successfully identified and mitigated.

List of used sources:

1. Методологія аналізу ризиків для підтримання рівня безпеки // Навч. посіб. Галак О., Писарєв С. ВІТВ НТУ «ХПІ». 2024. 160 с.

2. Галак О.В., Писарєв С.А., Матикін О.В. Аналіз можливого впливу на боєздатність підрозділів у разі застосування ядерної зброї / XXXI Міжнародної науково-практичної конференції MicroCAD-2023. С. 1292.

3. Галак О.В. Аналіз можливого впливу на боєздатність частин підрозділів у разі застосування ЗМУ та зруйнування об'єктів підвищеної небезпеки / Законодавчі аспекти протидії особливо небезпечним злочинам в Україні. С. 305–311.

ЩОДО ПИТАННЯ ТОКСИЧНОСТІ, ДЕГАЗАЦІЇ ТА УТИЛІЗАЦІЇ ПРОДУКТІВ ДЕГАЗАЦІЇ ІПРИТУ

Микола БЛАЖЕЄВСЬКИЙ
доктор хімічних наук, професор,
професор кафедри загальної хімії
Національного фармацевтичного університету
Міністерства охорони здоров'я України
Владислав ДЯДЧЕНКО
кандидат хімічних наук, доцент,
заступник начальника кафедри хімії
та бойових токсичних хімічних речовин
факультету радіаційного хімічного біологічного
захисту та екологічної безпеки
Військового інституту танкових військ
Національного технічного університету
«Харківський політехнічний інститут»

Сірчаний іприт (СІ) та подібні біфункціональні агенти використовувалися як хімічна зброя більше, як 100 років. З тих пір, як вони були вперше використані у війні в 1917 році, СІ та інші іприти були предметом інтенсивних досліджень, і їх хімія, фармакокінетика та механізми токсичної дії зараз досить добре вивчені [1].

Встановлено, що солі сульфонію роблять значний внесок у біологічну активність СІ, але продукти окиснення також можуть бути важливими [2].

Сульфоксид $[OS(CH_2CH_2Cl)_2]$ (СІО) є набагато менш реакційноздатним, ніж сульфон $[O_2S(CH_2CH_2Cl)_2]$, тому окиснення СІ до відповідного сульфоксиду вважається детоксикацією. За результатами досліджень СІО взагалі не мав цитотоксичних ефектів до тестованих концентрацій 10,25 мМ [3]. Під час розкладення сульфонового похідного СІ видаляється HCl з сульфону, утворюючи дивінілсульфон, який чутливий до нуклеофільної атаки з боку фрагмента X (рис. 1).

$$(ClCH_2CH_2)_2SO_2 \rightarrow (CH_2{=}CH)_2SO_2 + 2\ HCl$$
$$\downarrow\uparrow HX$$
$$(XCH_2CH)_2SO_2$$

Рис. 1 Схема реакції розкладення сульфонового похідного СІ.

Тому, як альтернативний варіант дегазації СІ, розглядається метод хімічної обробки пероксикарбоновими кислотами, який ґрунтується на реакції окиснення СІ до нетоксичного сульфоксиду:

$$S(CH_2CH_2Cl)_2 + RCO_3H \rightarrow O{=}S(CH_2CH_2Cl)_2 + RCO_2H.$$

З іншого боку, проблема утилізації сильнодіючих отруйних речовин і, зокрема, технічних СІ, що знаходяться на складах, тісно пов'язана з вирішенням низки проблем. Перш за все, необхідно вирішити питання про доцільність використання відходів. Практично всі запропоновані до теперішнього часу методи детоксикації іприту передбачають утилізацію продуктів відповідних хімічних реакцій.

Перспективним напрямком утилізації продукту детоксикації іприту пероксикарбоновими кислотами – відповідного сульфоксиду – є генерація інгібіторів окиснення нафтопродуктів [4].

Біс(2-хлоретил)сульфоксид можна використовувати для синтезу полісульфідів, або він може бути перетворений на тіоли під дією натрій полісульфіду:

$$O=S(CH_2CH_2Cl)_2 + nNa_2S_4 \rightarrow Na_2\text{-}[-SCH_2CH_2S(O)CH_2CH_2S_2\text{-}S\text{-}]n\text{-}SNa \rightarrow$$
$$\rightarrow (HCl/H_2O)HS_3\text{-}[-SCH_2CH_2S(O)CH_2CH_2S_2\text{-}S\text{-}]n\text{-}SH.$$

Спосіб реалізований в односторонньому процесі з практично повним перетворенням вихідного сульфіду. Сульфоксид може бути використаний як проміжний продукт синтезу олігосульфідосульфоксидів загальної формули $Na[-CH_2CH_2S(O)CH_2CH_2S\text{-}]n\text{-}SC(S)OC_4H_9$, які є ефективними сорбентами благородних металів.

Отже, спосіб дегазації сірчаного іприту за посередництвом пероксикислот є, безумовно, перспективним для впровадження його в практику.

Список використаних джерел:

1. Kamyar Ghabili, Paul S. Agutter, Mostafa Ghanei, Khalil Ansarin, Yunes Panahi, and Mohammadali M. Shoja. Sulfur mustard toxicity: History, chemistry, pharmacokinetics, and pharmacodynamics. *Critical Reviews in Toxicology*, 2011; 41(5): 384–403 ISSN1040–8444 print/ISSN1547–6898 online DOI: 10.3109/10408444.2010.541224.

2. Francis GE, Richards DE, Wormall A. (1957). The mechanism of the reaction between di-(2-chloroethyl) sulphone (mustard-gas sulphone) and amino acids. Biochem J 66:142–144.

3. Tsoutsoulopoulos A, Brockmöller S, Thiermann H, Steinritz D. Comparison of the toxicity of sulfur mustard and its oxidation products in vitro. Toxicol Lett. 2020 Mar 15;321:69–72. doi: 10.1016/j.toxlet.2019.12.015. Epub 2019 Dec 18. PMID: 31863871.

4. Аникиенко Д.А., Кузьменко А.И. Металлокомплексный катализ обрыва цепей окисления сульфоксидов: Тез. докл. VI нефтехим. симпоз. Киев. (15–20 окт. 1990 г.). М.: Наука, 1990, 127 с.

МЕХАНІЗМИ ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ ЗБРОЇ МАСОВОГО УРАЖЕННЯ

Степан ВЄЛІКОВ
молодший викладач
Національного юридичного університету
імені Ярослава Мудрого

24 лютого 2022 р.– день, коли рф здійснила широкомасштабне вторгнення в Україну, тим самим розв'язав вперше за довгий час повноцінний континентальний конфлікт в Європі.

Дані дії з боку рф призвели до того, що система колективної безпеки, яка формувалася протягом останніх десятиліть зазнала значних змін. Вперше за тривалий час постала реальна загроза застосуванню ядерної стратегічної/тактичної зброї. Востаннє такий рівень загрози фіксувався у часи Холодної під час Карибської кризи.

За загальною практикою до зброї масового ураження (надалі – ЗМУ) відносять наступні види зброї – хімічна, біологічна та ядерна. Дані види зброї характеризуються надвеликою силою руйнування та ураження порівняно з іншими видами зброї.

Зброя масового ураження несе в собі жахливу загрозу для людства, адже її руйнівна сила може торкнутися не лише людей, а також довкілля, де вони живуть. Це стосується не лише клімату та географії, але й флори та фауни.

Жахливі наслідки застосування даного виду зброї не обмежуються моментом застосування. Фактори ураження продовжують діяти протягом тривалого часу, завдаючи шкоди не лише у момент вибуху чи викиду, але й протягом тривалого періоду.

Застосування ЗМУ може призвести до:

– тривалих проблем зі здоров'ям у людей, які зазнали впливу ЗМУ, що виразиться у стражданні від гострих та хронічних захворювань, а також може призвести до генетичних порушень;
– економічних збитків, викликаних руйнуванням інфраструктури та забруднення довкілля.

На сьогоднішній день існують міжнародні домовленості у сфері обмеження розробки, виробництва, використання та розповсюдження ЗМУ. Ці угоди відіграють важливу роль у забезпеченні міжнародної безпеки та стабільності.

До ключових міжнародних угод відносять:

1) Договір про нерозповсюдження ядерної зброї від 1 липня 1968 року (надалі – ДНЯЗ) [1];

2) Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення від 13 січня 1993 року (надалі – КХЗ) [2];

3) Конвенція про заборону розробки, виробництва, накопичення запасів бактеріологічної (біологічної) та токсинної зброї та про її знищення від 10 квітня 1972 року (надалі – КБТЗ) [3].

Відповідно до ст. 1 ДНЯЗ, кожна з держав-учасниць цього Договору, що володіє ядерною зброєю, зобов'язується не передавати будь-кому ядерну зброю або інші ядерні вибухові пристрої, а також контроль над такою зброєю чи вибуховими пристроями ні безпосередньо, ні посередньо, рівно як і ніяким чином не допомагати, не заохочувати і не спонукати будь-яку державу, що не володіє ядерною зброєю, до виробництва або придбання у будь-який інший спосіб ядерної зброї чи інших ядерних вибухових пристроїв.

Відповідно до ст. 2 ДНЯЗ, кожна з держав-учасниць цього Договору, що не володіє ядерною зброєю, зобов'язується не приймати передачі від кого б то не було ядерної зброї чи інших ядерних вибухових пристроїв.

З вищевикладеного виходить, що даною Угодою фіксується перелік країн, які мають в своєму розпорядженні ядерні технології та ядерну зброю, а підписанти Угоди, в свою чергу, зобов'язуються не розповсюджувати ядерну зброю та не приймати її від інших держав. Угода також передбачає заходи щодо скорочення ядерних озброєнь та запобігання ядерній війні.

Відповідно до преамбули КХЗ, держави-учасниці цієї Конвенції, сповнені рішучості діяти з метою досягнення ефективного прогресу у напрямку загального та повного роззброєння під суворим та ефективним міжнародним контролем, включаючи заборону та ліквідацію усіх видів зброї масового знищення.

Відповідно до ст. 1 КХЗ, Кожна держава-учасниця цієї Конвенції зобов'язується ніколи, ні за яких умов:

a) не розробляти, не виробляти, не придбавати іншим чином, не накопичувати або не зберігати хімічну зброю або не передавати прямо чи непрямо хімічну зброю будь-кому;

b) не застосовувати хімічну зброю;

c) не проводити будь-яких військових підготувань до застосування хімічної зброї;

d) не допомагати, не заохочувати або не спонукати будь-яким чином будь-кого до будь-якої діяльності, яка забороняється державі-учасниці цією Конвенцією.

Угода також передбачає знищення всіх запасів хімічної зброї державами-учасницями.

Держави, які приєдналися до КБТЗ, зобов'язуються не займатися розробкою, виробництвом, придбанням чи зберіганням особливо небезпечних мікроорганізмів. Ці мікроорганізми становлять загрозу для людей, тварин та рослин, і їх використання не повинно виходити за рамки мирних цілей, таких як наукові дослідження, профілактика хвороб, захисні заходи та інші подібні дії. Додатково, Конвенція забороняє розробку та зберігання обладнання та засобів доставки, призначених для застосування цих мікроорганізмів у збройних конфліктах або з будь-якими злочинними намірами.

Будь-який нормативно-правовий акт, в тому числі й міжнародний, повинні бути забезпечені механізмом санкції задля підкреслення рішучості, послідовності та невідворотності досягнення мети, визначеною в акті. Саме тому, механізм санкцій відіграє вирішальну роль у забезпеченні дотримання міжнародних договорів по нерозповсюдженню ЗМУ.

Санкції можуть бути застосовані до держав або окремих осіб, які порушують ці договори. В залежності від суб'єкта, який вчинив порушення міжнародних Угод, санкції можуть бути дипломатичними, економічними, військовими. А тому, застосування санкцій може бути потужним інструментом для примушування держав до дотримання Угод по нерозповсюдженню ЗМУ.

Окремо слід виділити такий механізм протидії розповсюдженню ЗМУ як – експортний контроль. Сучасні процеси глобалізації призвели до значного зростання міжнародної торгівлі товарами та технологіями. Це, з одного боку, сприяло економічному зростанню та розвитку, але з іншого боку, створило нові виклики для режиму нерозповсюдження (ЗМУ) та контролю за експортом. З метою вирішення цих проблем держави посилили режими експортного контролю.

Відповідно до ст. 4 Закону України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання», державна політика в галузі державного експортного контролю формується відповідно до таких основних принципів – забезпечення взаємодії з міжнародними організаціями та іноземними державами в галузі державного експортного контролю з метою зміцнення міжнародної безпеки і стабільності, у тому числі з метою запобігання розповсюдженню зброї масового знищення та засобів її доставки [4].

З вищевикладеного доходимо висновку, що в умовах сьогодення протидія розповсюдженню ЗМУ має вкрай важливе значення, з огляду на геополітичну ситуацію, що склалася в світі. Вторгнення рф в Україну стало нагадуванням про те, що загроза застосування ЗМУ залишається актуальною. Саме тому, міжнародне співтовариство повинне й надалі докладати зусиль для посилення режиму нерозповсюдження ЗМУ та запобігання його використанню через оновлення та впровадження нових механізмів протидії цьому.

Список використаних джерел:

1. Договір про нерозповсюдження ядерної зброї від 1 липня 1968 року. Ратифіковано Законом України № 248/94-ВР від 16.10.98. URL: https://zakon.rada.gov.ua/laws/show/995_098#top (дата звернення: 17.06.2024).

2. Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення. Ратифіковано Законом України N187-XIV (187–14) від 16.10.98. URL: https://zakon.rada.gov.ua/laws/show/995_182#Text (дата звернення: 17.06.2024).

3. Конвенція про заборону розробки, виробництва, накопичення запасів бактеріологічної (біологічної) та токсинної зброї та про її знищення від 10 квітня 1972 року. Ратифікована Українською РСР 21.02.75 р. URL: https://ips.ligazakon.net/document/MU71K09U (дата звернення: 17.06.2024).

4. Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання». URL: https://zakon.rada.gov.ua/laws/show/549–15#top (дата звернення: 17.06.2024).

СУДОВО-ЕКСПЕРТНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ РХБЯ ЗАГРОЗАМ

Юрій ВОЗОВИК
співробітник СБУ

З урахуванням наявності фактів систематичного застосування підрозділами російської федерації токсичних хімікатів проти підрозділів сил оборони України, наявністю реальної загрози застосування російською федерацією проти сил оборони України ядерної зброї, питання судово-експертного забезпечення в частині дослідження радіоактивних, хімічних, біологічних

та ядерних (надалі – РХБЯ) матеріалів є досить актуальним для забезпечення завдань з документування, розслідування та притягнення до відповідальності як на національному, так і на міжнародному рівнях за злочини, пов'язані з застосуванням ядерної, хімічної та біологічної зброї.

Під час розслідування вказаних злочинів виявляються факти використання країною-агресором хімічної зброї, яка заборонена Конвенцією [1]. Тільки з відкритих джерел відомо, що у період з лютого 2023 року по квітень 2024 року підрозділи російської федерації 1891 разів використали проти сил оборони України боєприпаси, споряджені небезпечними хімічними речовинами [2].

Слід зазначити, що відповідно до статті 216 Кримінального процесуального кодексу України [3] слідчі органів безпеки здійснюють досудове розслідування злочинів, передбачених статтею 438 Кримінального кодексу України [4] «Порушення законів та звичаїв війни», статтею 439 Кримінального кодексу України [4] «Застосування зброї масового знищення», статтею 440 Кримінального кодексу України [4] «Розроблення, виробництво, придбання, зберігання, збут, транспортування зброї масового знищення», статтею 441 Кримінального кодексу України [4] «Екоцид».

Відповідно до Закону України [5], виключно державними спеціалізованими установами здійснюється судово-експертна діяльність, пов'язана з проведенням криміналістичних, судово-медичних і судово-психіатричних експертиз. До державних спеціалізованих установ, серед інших, належить експертна служба Служби безпеки України.

Відповідно до Статуту [6], Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України (надалі – ІСТЕ СБУ) є державною спеціалізованою експертною науково-дослідною установою, яка здійснює, зокрема, судову експертну діяльність та виконує функції експертної служби Служби безпеки України. До основних завдань ІСТЕ СБУ, серед інших, належать судово-експертне забезпечення діяльності підрозділів та органів Служби безпеки України, інших правоохоронних органів та суду.

Відповідно до Положення [7], ІСТЕ СБУ є головним суб'єктом Експертної служби Служби безпеки України, одним із завдань якої є здійснення судово-експертної діяльності, проведення судової експертизи в кримінальному та виконавчому провадженнях, адміністративних, цивільних і господарських справах, справах про адміністративні правопорушення.

З метою вдосконалення судово-експертного забезпечення діяльності підрозділів та органів Служби безпеки України, інших правоохоронних органів та суду у разі реагування на інциденти з РХБЯ речовинами, Перелік основних видів судових експертиз та експертних спеціальностей, за якими присвоюється кваліфікація судового експерта фахівцям експертних підрозділів Служби безпеки України Положення [8], доповнено новими видами експертних спеціальностей: 8.19 «Дослідження радіоактивних та ядерних матеріалів», 8.20 «Дослідження матеріалів хімічної зброї та 8.21 «Дослідження матеріалів біологічної зброї». Проведення вказаних досліджень передбачено в рамках судової експертизи матеріалів, речовин та виробів.

Слід відмітити, що серед державних спеціалізованих установ, які здійснюють судово-експертну діяльність, експертні спеціальності, пов'язані з дослідженнями РХБЯ матеріалів, введено в Україні вперше.

На теперішній час дослідження ізотопного складу і спектрометричного аналізу радіоактивних та ядерних матеріалів здійснює Інститут ядерних досліджень Національної академії наук України, який є головною експертною організацією з питань дослідження та визначення характеристик радіоактивних матеріалів, які вилучено з незаконного обігу [9]. Вказана установа не відноситься до державних спеціалізованих установ, які здійснюють судово-експертну діяльність, відтак, не може проводити криміналістичні види досліджень. Аналогічна ситуація склалася в частині дослідження матеріалів хімічної та біологічної зброї.

Відсутність в Україні визнаних на міжнародному рівні лабораторій, які відповідають вимогам законодавства України та здатні проводити судово-експертні дослідження РХБЯ матеріалів, негативно впливає на забезпечення завдань з документування, розслідування та при-

тягнення до відповідальності як на національному, так і на міжнародному рівнях за злочини, пов'язані з застосуванням ядерної, хімічної та біологічної зброї.

Для вирішення вказаної проблематики неодноразово підіймалося питання створення в Україні на базі вже існуючих державних спеціалізованих установ, які здійснюють судово-експертну діяльність, акредитованих (визнаних на міжнародному рівні) лабораторій, оснащених передовим обладнанням та забезпеченими висококваліфікованими фахівцями. У тому числі фахівцями, здатними проводити судово-експертні дослідження РХБЯ матеріалів.

Більшість думок сходиться на тому, що шляхом вирішення вказаної проблематики є створення та функціонування відповідних лабораторій на базі ІСТЕ СБУ. Адже розуміючи гостру потребу у вдосконаленні спроможностей судово-експертного забезпечення в частині дослідження РХБЯ матеріалів, в ІСТЕ СБУ здійснено відповідні заходи, а саме: вперше введено експертні спеціальності, пов'язані з дослідженнями РХБЯ матеріалів, а також здійснюються заходи щодо навчання та стажування співробітників, які є судовими експертами, за напрямками досліджень РХБЯ матеріалів. Суттєвою перевагою судових експертів ІСТЕ СБУ є те, що судові експерти є військовослужбовцями, які можуть виконувати службові обов'язки в небезпечних умовах.

Слід зазначити, що в рамках експертних спеціальностей 8.11 «Дослідження речовин хімічних виробництв та спеціальних хімічних речовин» та 8.13 «Дослідження сильнодіючих і отруйних речовин» судової експертизи матеріалів, речовин та виробів, в ІСТЕ СБУ вже проводяться судові експертизи матеріалів, речовин та виробів з дослідження речовин, які можуть бути використані в якості хімічної зброї. Вказані дослідження стосуються переважно отруйних речовин подразнюючої дії. Оскільки в ІСТЕ СБУ відсутні стандартні зразки речовин, які включені до Списків 1, 2, 3 Конвенції [1], проведення досліджень повного кола речовин хімічної зброї в установі обмежено. Окрім того, з початку поточного року в ІСТЕ СБУ виконано 35 судових експертиз щодо об'єктів пов'язаних із застосуванням хімічної зброї підрозділами рф проти сил оборони України (речовин призначених для боротьби із заворушеннями, які відповідно до пункту 5 статті 1 Конвенції [1].

Із наведеного вище можливо зробити висновок, що вдосконалення судово-експертного забезпечення протидії РХБЯ загрозам є невід'ємною частиною інноваційної стратегії забезпечення національної безпеки. Створення та функціонування на базі ІСТЕ СБУ лабораторії з досліджень РХБЯ матеріалів повною мірою забезпечить виконання заходів з документування, розслідування та притягнення до відповідальності як на національному, так і на міжнародному рівнях за злочини, пов'язані з застосуванням РХБЯ матеріалів.

Список використаних джерел:

1. Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення від 13.01.1993, ратифікована Законом України від 16 жовтня 1998 року № 187-XIV. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995–182#Text (дата звернення: 13.06.2024).

2. Росія у квітні 444 рази застосувала хімічні боєприпаси проти ЗСУ,– Генштаб espreso.tv: веб-сайт. URL: https://www.google.com/amp/s/espreso.tv/viyna-z-rosiyeyu-rosiya-u-kvitni-444-razi-zastosuvala-khimichni-boepripasi-proti-zsu-gensht ab%3famp (дата звернення: 13.06.2024).

3. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text (дата звернення: 13.06.2024).

4. Кримінальний кодекс України: Закон України від 05 квітня 2001 року

№ 2341-III. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text (дата звернення: 13.06.2024).

5. Про судову експертизу: Закон України від 13 квітня 2012 року № 4651-VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text (дата звернення: 13.06.2024).

6. Статут Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України в новій редакції: наказ Центрального управління Служби безпеки України від 01 березня 2023 року № 73.

7. Положення про Експертну службу Служби безпеки України: наказ Центрального управління Служби безпеки України від 05 червня 2024 року № 264.

8. Положення про експертно-кваліфікаційну комісію Служби безпеки України та атестацію судових експертів: наказ Центрального управління Служби безпеки України від 24 грудня 2014 року № 855. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z0044–15#Text (дата звернення: 17.06.2024).

9. Порядок взаємодії органів виконавчої влади та юридичних осіб, які провадять діяльність у сфері використання ядерної енергії, в разі виявлення радіоактивних матеріалів у незаконному обігу: Постанова Кабінету Міністрів України від 02 червня 2003 року № 813. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/813–2003-%D0%BF#Text (дата звернення: 19.06.2024).

CHEMICAL WEAPONS AND CHEMICAL TERRORISM

Oleksandr HALAK
Candidate of Technical Sciences, Associate Professor
Head of the Department of CBRN Protection
of the Faculty of CBRN Defence and
Environmental Safety of the Military
Institute of Tank Forces of NTU ‘KhPI’

Since the use of chemical agents during World War I, CBRN threats have continuously evolved, as seen in the use of nerve agents by terrorists in Japan, and the recent resurgence of use by state actors, notably in Syria and for assassination attempts in the UK.

Over the last century, CBRN threats have moved from the battlefield to the civilian environment and now pose a significant and real threat to civilians. The COVID-19 pandemic demonstrates the unpredictable nature of the chemical, biological, radiological and nuclear (CBRN) environment that NATO faces. In addition to the pandemic, NATO and its member states must be prepared to address the full spectrum of CBRN threats and hazards, from man-made disasters to bioterrorism and the proliferation or use of weapons of mass destruction.

The recent removal of dangerous chemical weapons precursors from Libya has prevented the Islamic State group from adding these horrific weapons to its arsenal of terror. Libya’s Government of National Accord requested the assistance of the Organisation for the Prohibition of Chemical Weapons, as it feared that Islamic State fighters were advancing towards a facility containing these deadly chemicals. Preventing the Islamic State group from adding deadly chemicals to its horrific weapons cache in Libya is a critical success in the fight against terrorism.

US Director of National Intelligence James Clapper said in congressional testimony that the use of chemical warfare agents by the Islamic State group in Syria is the first time a terrorist group has demonstrated such a capability since the Japanese cult Aum Shinriko used sarin gas in the Tokyo subway in 1995. After the Tokyo attack, terrorists crashed passenger planes into the World Trade Towers and took schoolchildren hostage on the first day of September in Beslan. Terrorists have certainly talked about using poison, disease and radioactivity as weapons, but in general they have pursued other targets that are more readily available and easier to deploy.

In Syria and Iraq, the Islamic State and Al-Nusra The United Nations Commission of Inquiry on the Use of Chemical Weapons in Syria reported that it had found evidence that the Islamic State and Al-Nusra Front had acquired and used chemical weapons.

The United States and coalition partners fighting both groups have bombed storage and production facilities for chemical weapons of the suspected Islamic State group. Earlier, US Air Force Lieutenant General Jeffrey Harrigian said at a press conference that coalition forces had struck a pharmaceutical plant that the Islamic State group was using to produce chemicals. For the time being, this will certainly limit the Islamic State and Nusra Front's efforts to produce chemical weapons, but the long-term impact is uncertain.

But what has motivated these groups to do something that no other terrorist organisation has done in the past 21 years? In short, the opportunity When the Islamic State and Nusra Front groups seized territory in Syria and northern Iraq, they stumbled upon military installations where chemical munitions were hidden, abandoned or lost. In addition to seizing territory, they also took over industrial facilities using toxic chemicals. When these toxic capabilities became available, they exploited them. Unfortunately, the victims of these indiscriminate weapons were usually innocent civilians.

The Islamic State and Al-Nusra Front not only used captured weapons resources, but also took the opportunity to develop some of their own capabilities. Just as al-Qaeda once had a safe haven in Taliban-controlled Afghanistan, the Islamic State and Al-Nusra Front have had the freedom to develop capabilities in Islamic State-controlled territory and ungoverned spaces that neither the Syrian nor Iraqi governments can control.

Intelligence agencies of Ukraine's allies have repeatedly claimed that the Russian Federation is likely planning to use CBRN weapons in Ukraine. By spreading false information about biological laboratories in Ukraine where the Pentagon allegedly developed biological weapons, Moscow wants to prepare the ground for further escalation of its unjustified military aggression in Ukraine. Russia's accusations that Ukraine intends to use chemical and biological weapons continue unabated. Allied intelligence indicates that it is highly unlikely that the Russian Federation would use CBRN weapons and that a false flag operation could be organised, and Russian officials fantasise about non-existent chemical weapons in Ukraine with 'manic obsession'. Russia has a clear pattern of behaviour – it is either preparing to use weapons of mass destruction itself or planning to stage an attack by the Ukrainian armed forces to create a pretext for a symmetrical response and prolong the war.

The international community is aware of the dangers of chemical weapons. For a century, humanity has been actively fighting for the prohibition of chemical weapons in an effort to prevent the dangerous consequences of their use. However, there are still many possible sources of chemical hazards. These may include terrorist acts, related or deliberate accidents at chemical plants, aggression by a state uncontrolled by the international community, etc. At the same time, the danger of uncontrolled proliferation and use of chemical weapons, the realisation that large volumes of accumulated toxic substances pose a great threat in themselves due to the difficulties of ensuring the safety of their storage, is an urgent problem today.

That is why the Centre for Countering Disinformation has to refute the information that there are laboratories in Ukraine where chemical weapons are allegedly produced. The Russian State Council Of course, Russian propagandists have not been able to provide evidence of the existence of such biological laboratories.

Russian Federation troops in the area of combat missions, against Ukrainian defence forces units, drop a RG-VO 862–7–23 munition containing a chemical substance from an enemy quadcopter.

List of used sources:

1. Методологія аналізу ризиків для підтримання рівня безпеки // Навч. посіб. Галак О., Писарєв С. ВІТВ НТУ «ХПІ». 2024. 160 с.

2. Галак О.В., Чулінда А.А., Топчий В.Л. Аналіз можливого впливу на боєздатність підрозділів у разі застосування хімічної зброї в районі бойових дій / XXXI Міжнародної науково-практичної конференції MicroCAD-2023. С. 1293.

3. Галак О.В. Аналіз можливого впливу на боєздатність частин підрозділів у разі застосування ЗМУ та зруйнування об'єктів підвищеної небезпеки / Законодавчі аспекти протидії особливо небезпечним злочинам в Україні. С. 305–311.

ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ В СФЕРІ ФІЗИЧНОГО ЗАХИСТУ, ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В БОРОТЬБІ З РАДІАЦІЙНИМИ ЗАГРОЗАМИ

Сергій ДРАПЕЙ
кандидат фізико-математичних наук,
завідувач Навчального центру з фізичного захисту
обліку та контролю ядерних матеріалів імені Джоржа Кузмича
Інституту ядерних досліджень НАН України, Київ

Кабінет Міністрів України розпорядженням від 03.09.97 № 488-р на Інституті ядерних досліджень НАН України (ІЯД) поклав організацію та проведення навчальної підготовки з підвищення кваліфікації спеціалістів, причетних до обліку й контролю ядерних матеріалів, фізичного захисту ядерних установок, ядерних матеріалів. Уряд США відповідно до закону Нанна-Лугара надав допомогу ІЯД у створенні й оснащенні Навчального центру з підвищення кваліфікації вищезазначених фахівців. За роки свого функціонування з 1998 року було створено розвинену унікальну навчально-тренувальну базу, до складу якої входять: відкритий навчально-тренувальний майданчик «Комплекс інженерно-технічних засобів системи фізичного захисту»; інтерактивний навчальний комплекс «АЕС з елементами фізичного захисту» і багатофункціональний корпус ситуаційних вправ, закінчений будівництвом у січні 2021 року.

Для забезпечення високого рівня ядерно-фізичної захищеності, держава створює та підтримує відповідний кадровий потенціал у сфері фізичної ядерної безпеки. На даний момент часу в Україні підвищення кваліфікації фахівців у сфері фізичної ядерної безпеки здійснює єдиний у країні Навчальний центр з фізичного захисту, обліку та контролю ядерного матеріалу ім. Дж. Кузмича ІЯД НАН України (далі – НЦДК).

НЦДК має дві ліцензії для здійснення підвищення кваліфікації з фізичного захисту, обліку та контролю ядерного матеріалу – ліцензіям Міністерства освіти і науки України та ліцензія Державної інспекції ядерного регулювання України.

Підвищення кваліфікації проходить відповідно до розроблених та пого-джених програм – 12, 20, 36, 72 та 144 години. На даний момент часу Навчальним центром розроблено та запроваджено більше 300 навчальних курсів у сфері фізично-ядерної безпеки.

Майданчики навчального центра залучаються міжнародними і державними органами для проведення навчань, міжнародних науково-технічних семінарів та конференцій, як для цивільних структур так і для силового блоку країни. За роки своєї діяльності підвищення кваліфікації у навчальному центрі пройшли близько 7600 слухачів з 160 організацій України крім того близько 800 представників збільше як 30 іноземних держав та міжнародних організацій.

НЦДК співпрацює і планує продовжувати співпрацю з Національним технічним університетом України «Київський політехнічний інститут імені Ігоря Сікорського» (підготовка фахівців з фізичної ядерної безпеки), Академією СБУ (розробка навчальних програм і підготовка кадрів), Академією Національної гвардії України (розробка навчальних програм, підготовка кадрів і читання лек-цій), Академією Національної поліції України (розробка навчальних програм, підготовка кадрів і читання лекцій), Міненерго (підготовка фахівців з фізичного захисту, обліку й контролю ядерних матеріалів), Національною гвардією України (підготовка фахівців особового складу НГУ, який виконує завдання з охорони ядерних установок, ядерних матеріалів і спеціальних вантажів), АТ НАЕК «Енергоатом» (підготовка фахівців з фізичного захисту, обліку й контролю ядерних матеріалів і персоналу, який забезпечує експлуатацію ядерних установок, використання і зберігання ядерних матеріалів), правоохоронними органами, до повноважень яких належить здійснення заходів фізичного захисту (навчання та підвищення кваліфікації співробітників відповідних підрозділів правоохоронних органів), ДСП «Об'єднання Радон» (підвищення кваліфікації фахівців з фізично-го захисту), медичними закладами (під-

вищення кваліфікації фахівців з фізичного захисту джерел іонізуючого випромінювання), Державною установою «Центр громадського здоров'я Міністерства охорони здоров'я України» (підвищення кваліфікації фахівців з фізичного захисту джерел іонізуючого випромінювання та реагування на кризові й надзвичайні ситуації), Адміністрацією Державної прикордонної служби України (підготовка фахівців особового складу ДПСУ), Розрахунково-аналітичним центром Збройних Сил України (підготовка фахів-ців), Управлінням військ РХБ захисту Командування Сил підтримки Збройних Сил України (підготовка фахівців, розробка інструкцій, регламентів тощо), ДЗ «Український науково-практичний центр екстреної медичної допомоги та меди-цини катастроф Міністерства охорони здоров'я України» (підготовка фахівців), Інститутом державного управління та наукових досліджень з цивільного захисту (підготовка фахівців, участь у розробці нормативних документів, спільна науко-ва діяльність тощо.

Після перевірки знань та успішного складання екзаменаційної роботи здо-бувачу освіти видається свідоцтво про підвищення кваліфікації, зразок якого за-тверджено наказом директора ІЯД НАН України № 43 від 11 квітня 2016 р.

Список використаних джерел:

1. Закон України 2064-III «Про фізичний захист ядерних установок, ядерних ма-теріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання». Відомості Верховної Ради України (ВВР). 2001. № 1. Ст. 1

2. Про затвердження Положення про державну систему професійної підготовки, перепідготовки та підвищення кваліфікації фахівців з фізичного захисту, обліку та контролю ядерних матеріалів: постанова Кабінету Міністрів України від 21 березня 2012 р. № 263// Офіційний вісник України.– 2012.– № 25 – стор.14 – Ст. 949.

3. Educational Programme in Nuclear security (Technical Guidance): IAEA Nuclear Security Series № 12 / IAEA – Vienna, 2010/ Офіційний сайт МАГАТЕ – [Елект-ронний ресурс].– Режим доступу: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1439_web.pdf. (Дата звернення 20.06.2024)

ПРЕДМЕТ ТА ЗАВДАННЯ СУДОВОЇ ЕКСПЕРТИЗИ ЗА НАПРЯМОМ ДОСЛІДЖЕННЯ РАДІОАКТИВНИХ ТА ЯДЕРНИХ МАТЕРІАЛІВ

Халіл КАЛТАЄВ
кандидат технічних наук,
співробітник СБУ

Впровадження в судову експертну діяльність судової експертизи матеріалів, речовин та виробів за експертною спеціальністю 8.19 «Дослідження радіоактивних та ядерних матеріалів» викликане необхідністю вдосконалення можливостей судово-експертного забезпечення діяльності підрозділів та органів Служби безпеки України, враховуючи зростаючу загрозу неконтрольованого розповсюдження та використання радіоактивних та ядерних матеріалів в злочинних цілях, у тому числі у злочинах проти людства. Розкриття предмета та завдань досліджень судової експертизи за експертною спеціальністю «Дослідження радіоактивних та ядерних матеріалів» необхідне для відмежування її від інших класів і родів експертиз, розуміння кола питань, які вона вирішує.

Для розкриття предмета судової експертизи за експертною спеціальністю «Дослідження радіоактивних та ядерних матеріалів» необхідно систематизувати класифікаційні, ідентифікаційні та діагностичні задачі, які вирішуються відповідним судово-експертним дослідженням.

Класифікаційною задачею є визначення природи об'єктів, тобто віднесення їх до радіоактивних та ядерних матеріалів. Предметом дослідження класифікаційної задачі, на підставі якої об'єкт дослідження буде віднесений до радіоактивних матеріалів, є його здатність до α-, β-, γ-, нейтронного випромінювання. Радіоактивний матеріал у свою чергу класифікується як ядерний, якщо до його складу входять ізотопи плутонія-239, урану-233, урану-235 [1]. Предметом дослідження у цьому випадку є належність до ізотопів з певними атомними масами.

Предметом дослідження підмножини класифікаційних задач по встановлення типу виробу з радіоактивного або ядерного матеріалу є визначення його функціонального призначення – паливні елементи атомної електростанції, калібровані джерела іонізуючого випромінення в геодезичних або медичних приладах тощо. Вирішення такої задачі потребує порівняльних зразків виробів (або їх візуального відображення). У деяких випадках віднесення матеріалу до певного класу має самостійне доказове значення, утворюючи суттєвий елемент предмету доказування. Наприклад, віднесення наданого на дослідження об'єкту до збройового плутонію-239 є підставою для відкриття кримінальної справи по факту незаконного заволодіння та розповсюдження ядерного матеріалу з атомної електростанції з реактором великої потужності канальним (РВПК).

Для об'єктів судової експертизи за експертною спеціальністю 8.19 «Дослідження радіоактивних та ядерних матеріалів» характерні три види індивідуальної ідентифікації: ідентифікація ізотопу, цілого по окремим частинам і конкретного джерела походження.

Ідентифікація радіоактивного ізотопу проводиться за унікальними для кожного ізотопу характеру та енергії випромінювання (наприклад, ізотоп цезій-137 ідентифікується за β-випромінюванням з енергією електронів 1,17563 МеВ [2]).

Ідентифікація цілого за частинами при дослідженні радіоактивних чи ядерних матеріалів проводиться за ізотопним складом. Об'єктами дослідження можуть бути зруйновані тепловиділяючі елементи, залишки непрореагованого збройового плутонію-239 після ядерного вибуху. При цьому ідентифікуючою ознакою є однакове співвідношення материнського та дочірнього ізотопу в об'єктах дослідження.

Під джерелом походження в судовій експертизі матеріалів, речовин та виробів за експертною спеціальністю «Дослідження радіоактивних та ядерних матеріалів» мається на увазі місце виготовлення, видобування (у разі дослідження руд, які містять радіоактивні елементи), зберігання, експлуатації, перебування об'єктів. Джерело походження об'єктів за місцем їх видобування або виготовлення може бути встановлене за специфічними домішками та ізотопним складом. Під місцем походження розуміються також реактори атомних електростанцій. Радіоактивні чи ядерні матеріали мають специфічний ізотопний склад відповідно до типу реактору, в якому вони був напрацьовані.

Завдання встановлення джерела виготовлення виробу з радіоактивного чи ядерного матеріалу принципово може бути вирішене за умови доступу до інформаційного фонду, в якому зібрані відомості про підприємства, які виробляють специфічні радіоактивні або ядерні матеріали (асортимент продукції та її призначення, сировина, яка використовується, технологічні режими та інше).

Вирішенням діагностичної задачі може бути встановлений час з моменту утворення материнського ізотопу. Предметом дослідження є належність до певного ізотопу з відомою сталою напіврозпаду та співвідношення материнського та дочірнього ізотопу в матеріалі, який досліджується.

На відміну від інших видів судової експертизи матеріалів, речовин та виробів, в яких ідентифікаційні та діагностичні властивості об'єктів задані будовою та станом електронних оболонок їх атомів, для ідентифікації та діагностування об'єктів дослідження судової експертизі матеріалів, речовин та виробів за експертною спеціальністю 8.19 «Дослідження радіоактивних та ядерних матеріалів» використовуються властивості атомних ядер, а саме характер розпаду ядра (α-розпад, β-розпад), наявність, інтенсивність та енергія γ- та нейтронного випромінювання.

Список використаних джерел:

1. Про використання ядерної енергії та радіаційну безпеку: Закон України від 08 лютого 1995 року № 39/95-ВР. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/39/95-%D0%B2%D1%80#Text (дата звернення: 18.06.2024).

2. Audi G., Wapstra A.H., Thibault C. The AME2003 atomic mass evaluation (II). Tables, graphs and references. Nuclear Physics A.– 2003.– Vol. 729.– P. 337–676.

ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ АНТИТЕРОРИСТИЧНОГО ЦЕНТРУ ПРИ СЛУЖБІ БЕЗПЕКИ УКРАЇНИ З ПИТАНЬ ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ ТА ЗАСТОСУВАННЮ РАДІАЦІЙНОЇ, ХІМІЧНОЇ, БІОЛОГІЧНОЇ ТА ЯДЕРНОЇ ЗБРОЇ

Олександр КОЗЕНКО
кандидат юридичних наук,
співробітник СБУ

Боротьба з тероризмом є актуальною проблемою сьогодення, нагальним завданням не лише правоохоронних органів, але й інших державних органів, справою інститутів громадського суспільства. Ефективність цієї діяльності зумовлена якістю законодавчого забезпечення цього процесу, наявністю оптимальних технологій протидії та правильною побудовою системи органів, що мають їх реалізовувати, а тому міжнародний досвід є вкрай важливим для України з точки зору пошуку своєї найбільш ефективної моделі протидії, так і об'єднання зусиль з провідними розвинутими країнами у цьому напрямку.

На Антитерористичний центр при Службі безпеки України (далі – АТЦ при СБУ) покладається участь у підготовці проектів міжнародних договорів України, підготовка і подання в установленому порядку пропозицій щодо вдосконалення законодавства України у сфері боротьби з тероризмом, фінансування проведення суб'єктами, які ведуть боротьбу з тероризмом, антитерористичних операцій, здійснення заходів щодо запобігання, виявлення та припинення терористичної діяльності.

Поточну роботу з виконання завдань, покладених на АТЦ при СБУ, організовує його Штаб, стаття 7 Закону України «Про боротьбу з тероризмом» [1].

Важливе значення у сфері протидії тероризму має реалізація спеціальних проектів (програм) та ініціатив іноземних держав, наприклад, під егідою Державного департаменту США.

У Департаменті функціонує Бюро з протидії тероризму та насильницькому екстремізму, що займаються розробкою скоординованих стратегій та підходів до боротьби з тероризмом за кордоном та забезпечує антитерористичне співробітництво міжнародних партнерів [2].

Окрім того, для реалізації програм технічної допомоги та перевірок виконання угоди з контролю над озброєнням в Україні функціонує Офіс Агентства зі зменшення загрози у сфері оборони, який є Координаційним центром Міністерства оборони США (далі – Агентство).

На засіданні Глобального партнерства у листопаді 2014 Уряд України висунув кілька пропозицій з проханням допомоги у сфері ядерної та радіологічної безпеки, а також прохання про поліпшення засобів контролю і реагування на ядерні інциденти. У відповідь на це та з метою надання необхідного обладнання та підвищення професійної підготовки особового складу, по-

силення спроможностей виконання завдань, покладених на підрозділи Національної поліції України, Національної гвардії України та Служби безпеки України (далі – СБУ) у сфері незаконного обігу ядерних матеріалів Агентством реалізовано проект міжнародної технічної допомоги «Готовність України у сфері ядерної безпеки» (далі – проект) започаткований 27.01.2020 (реєстраційна картка проекту (програми) від 27.01.2020 № 4279).

Штаб АТЦ при СБУ здійснює (у якості реципієнта) заходи з реалізації проекту [3].

Формат проекту полягає в наданні іноземним партнером з розвитку силам реагування суб'єктів боротьби з тероризмом (насамперед профільним підрозділам правоохоронних органів) фахової методичної та методологічної підготовки за міжнародними стандартами, а також забезпечення сучасними зразками спеціалізованої техніки, засобів виявлення та ідентифікації радіоактивних матеріалів, комунікації, індивідуального захисту від впливу радіації, спорядження, обладнання, тощо.

За період реалізації проекту вдалось досягти:

– посилення спроможностей реагування на ядерні інциденти за напрямами радіаційний захист, виявлення, реагування, міжвідомча взаємодія;
– зниження ризиків особового складу СБУ при виконанні завдань (завдяки отриманню відповідних знань та сучасних зразків технічних засобів захисту і реагування);
– запозичення міжнародних практик протидії вчиненню правопорушень з використанням небезпечних хімічних, біологічних, радіологічних і ядерних (далі – ХБРЯ) матеріалів (під час навчальних заходів відпрацьовано алгоритми реагування та міжвідомчої взаємодії).

За рахунок проекту спільно з зацікавленими профільними підрозділами СБУ у 2020 році проведено самооцінку загального стану базової готовності (за наданою американськими партнерами методикою), та визначено потреби і обсяги військово-хімічного майна, необхідного для виконання покладених завдань з протидії ХБРЯ-терористичним посяганням, незаконному обігу радіоактивних матеріалів, та дотримання режиму нерозповсюдження зброї масового ураження. В період з червня 2021 по січень 2022 отримано обладнання (засоби індивідуального захисту, виявлення, ідентифікації, радіаційної розвідки, дозиметрії) на загальну суму 9,75 млн. грн. В подальшому (у продовж 2022–2024), у зв'язку з введенням в державі воєнного стану, матеріали, спорядження, приладний парк та інше майно відповідно до цілей проекту від партнера з розвитку проекту не отримувались.

Значна частина отриманого майна, у зв'язку з повномасштабною збройною агресією рф на території України та необхідністю виконання завдань з оборони держави від країни-агресора, (за рішенням керівництва) передана оперативно-бойовим підрозділам Центру спеціальних операцій по боротьбі з тероризмом, зберігається та належним чином використовується.

Окремим напрямом розвитку спроможностей відповідно до міжнародних стандартів НАТО передбачено функціонування інфраструктури технічної підтримки, обслуговування (калібрування приладного парку) та ремонту, яка в системі СБУ відсутня. Тому в майбутньому виникнуть потреби в отримання таких послуг від профільних організацій.

Поточна самооцінка розвитку спроможностей СБУ в рамках реалізації проекту проведена у березні-квітні 2024 за методичної підтримки іноземного партнера з розвитку із залученням усіх зацікавлених підрозділів і органів СБУ, на основі моніторингу зростаючих терористичних ХБРЯ-загроз.

Результати моніторингу повномасштабної збройної агресії російської федерації (далі – рф) на території України свідчить про наступне:

– тимчасово окуповано та розграбовано інфраструктуру Чорнобильської АЕС та об'єктів Чорнобильської зони відчуження;
– тимчасово окуповано й розграбовано Запорізьку АЕС, яка в комплексі з підривом дамби Каховської ГЕС, використовуються рф у якості інструменту ядерного шантажу міжнародної спільноти та України; окупаційна адміністрація несанкціоновано втручається в регламенти безпечної експлуатації Запорізької атомної станції; ворог системно руйнує лінії

електропередач Об'єднаної енергосистеми України, які живлять власні потреби систем безпеки цієї АЕС; рф декларує перезапуск ядерних реакторів без дотримання встановлених процедур ядерної безпеки та погрожує приєднанням до російської енергосистеми;
- пошкоджено споруду підкритичної ядерної збірки «Джерело нейтронів» ННЦ «Харківський науково-технічний інститут»;
- ракетно-дроновими та артилерійськими атаками знищується геодезичний полігон, комплексна лабораторія ННЦ «Інститут метрології» в пгт. Липці Харківської області, на якому зберігається велика кількість небезпечних радіоактивних джерел 1–2 категорії;

Одним з напрямів розвитку (посилення) спроможностей сил реагування на загрози ядерного тероризму в умовах воєнного стану також визначено забезпечення захищеності ядерних ОМТП та радіоактивних матеріалів. Пріоритетність обумовлена насамперед виробничими необхідностями:

АЕС України вивільняти басейни витримки від накопичень відпрацьованого ядерного палива шляхом вивезення до Центрального сховища, розташованого в Чорнобильській зоні відчуження;
- постачань з західноєвропейських країн до вітчизняних закладів медицини радіофармацевтичних препаратів для лікування онкозахворювань;
- підприємств, що використовують ядерні технології, вивозити радіоактивні відходи на тимчасове зберігання до регіональних сховищ спецкомбінатів «Радон».

Захищеність ядерних ОМТП та радіоактивних матеріалів від терористичних посягань забезпечується:
- у мирний час – проведенням (у форматі ТСН, КШН, тренувань) превентивних заходів з практичного відпрацювання алгоритмів координації, злагоджений дій, взаємодії та суміжності виконання завдань антитерористичної операції, а також визначення потреб у здійсненні заходів посилення захищеності спец перевезень ЯМ, РМ, удосконалень (уточнень) нормативних вимог, придбання сучасних зразків спецтехніки, технічних засобів, спорядження, озброєння тощо;
- в умовах воєнного стану (введеного Законом України «Про правовий режим воєнного стану» та Указом Президента України від 24.02.2022 № 64), враховуючи реальні ризики, та наявні спроможності забезпечення заходів радіаційної безпеки, обрано принцип виправданості кожного конкретного навчання, під час якого на практиці відпрацьовуються активні заходи з розвідки, захищеного оповіщення, РХБЯ-захисту, виявлення, ідентифікації та реагування на можливі загрози ворога [4, 5].

В даному контексті провадження проекту № 4279 розглядається як ефективний механізм запозичення кращих міжнародних практик з протидії загрозам ядерного та радіологічного тероризму. Відкриваються можливості впровадження методик, норм і стандартів контртерористичної діяльності країн НАТО.

Список використаних джерел:

1. Закон України «Про боротьбу з тероризмом» № 638-IV від 20 березня 2003 року – [Електронний ресурс].– Режим доступу: https://zakon.rada.gov.ua/laws/show/638–15#Text. (дата звернення: 18.06.2024)

2. Programs and Initiatives – U.S. Department of State. URL: https://www.state.gov/j/ct/programs/index.htm#ISEG. (дата звернення: 18.06.2024)

3. Реєстраційна картка проекту (програми) № 4279 «Готовність України у сфері ядерної безпеки».

4. Закон України «Про правовий режим воєнного стану» № 389-VIII від 12.05.2015 – [Електронний ресурс].– Режим доступу: https://zakon.rada.gov.ua/laws/show/389–219. (дата звернення: 18.06.2024)

5. Указ Президента України № 64 від 24.02.2022 – [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/642022–41397. (дата звернення: 18.06.2024)

ДО ОБГОВОРЕННЯ СТРАТЕГІЇ ЗАПОБІГАННЯ ЗАГРОЗАМ ВІД ЗБРОЇ МАСОВОГО УРАЖЕННЯ

Микола КОРЧАГІН
кандидат наук з фізичного виховання та спорту,
доцент, заслужений тренер України,
завідувач кфедри Національного юридичного
університету імені Ярослава Мудрого

У швейцарському Бюргенштоці завершився Саміт миру, на який прибули делегації з 92 країн та 8 світових організацій. Росію на нього не запросили, але, ймовірно, її покличуть на наступні – український президент вже анонсував проведення другого Саміту. За його словами, участь представників від росії «свідчитиме про бажання миру» [1]. На дводенному Саміті розглянули лише три з десяти пунктів української «Формули миру», які стосувалися ядерної та продовольчої безпеки й звільнення українських полонених і депортованих, зокрема, й дітей.

Один з ключових аспектів стратегії запобігання застосуванню росією ядерної зброї – це дипломатичні зусилля для забезпечення міжнародної стабільності та безпеки. Це включає в себе проведення міжнародних перемовин та укладення угод про обмеження збройних сил. Додатковою стратегією може бути розробка та підтримка систем раннього попередження про можливі загрози використання ядерної зброї, що дозволить своєчасно реагувати на кризові ситуації. Також важливою частиною стратегії може стати підтримка політики ядерного роззброєння та постійного моніторингу дотримання угод про недопущення поширення ядерної зброї.

Договір про нерозповсюдження ядерної зброї – багатосторонній міжнародний акт, розроблений Комітетом з роззброєння ООН з метою завадити розширенню кола держав, що мають ядерну зброю, забезпечити необхідний міжнародний контроль за виконанням державами узятих за умовами Договору зобов'язань щодо обмеження можливості виникнення збройного конфлікту із застосуванням такої зброї; створити широкі можливості для мирного використання атомної енергії. Договір схвалений Генеральною Асамблеєю ООН 12 червня 1968 і відкритий для підписання 1 липня 1968 року в Москві, Вашингтоні і Лондоні.

З 4 березня 2022 року, коли найбільша в Європі Запорізька атомна електростанція перебуває в російській окупації, кремль шантажує Україну і світ «мирним атомом» [3]. В травні 2023 року окупанти розмістили вибухівку в приміщенні турбінного відділення 4-го енергоблоку. На сьогодні вибухонебезпечною є вся територія станції, яку контролюють півтисячі військових країни-терориста.

Важливо зазначити, що реакція міжнародних організацій та країн на військову агресію залежить від конкретної ситуації, політичних обставин та правових рамок. Спільна дія та співпраця багатьох країн можуть допомогти запобігти військовій агресії та зміцнити світовий устрій [4].

З початком війни на Донбасі й згодом повномасштабного вторгнення питання ядерного роззброєння неодноразово обговорювали. Зауважують і те, що частину зброї, яку агресор використовує проти нас, Україна віддала йому в 90-х роках у межах Будапештського меморандуму [5].

Відновлення ядерного статусу для України означає відновлення її можливостей у галузі ядерної енергетики або ядерного озброєння. З моменту, коли Україна відмовилася від свого ядерного арсеналу в обмін на гарантії територіальної цілісності та безпеки від зовнішніх загроз у 1994 році, таке відновлення може бути важливим питанням для країни у зв'язку зі змінами у міжнародній ситуації та загрозами безпеки.

За підсумками дводенних дебатів на Саміті ухвалено підсумкову декларацію, яку підтримали 80 країн світу та 4 організації [6]. Першим пунктом є зазначене важливе: будь-яке використання ядерної енергії та ядерних установок має бути безпечним, захищеним, надійно охоронятися та не шкодити довкіллю. Українські атомні електростанції та установки, зокрема Запорізька атомна електростанція, повинні працювати безпечно та захищено під повним су-

веренним контролем України і відповідно до принципів МАГАТЕ та під її наглядом. Будь-яка загроза або використання ядерної зброї в контексті війни в Україні є недопустимими.

Отже, Україна робить значний крок на дипломатичному рівні щодо офіційного залучення багатьох країн Світу до проблематики застосування росією зброї масового ураження. Адже залученість у даний процес значної кількості країн наближують мир в Україні.

Список використаних джерел:

1. [Електронний ресурс]. Режим доступу https://suspilne.media/769701-ponad-90-krain-ucasnic-spilne-komunike-ta-pidgotovka-do-nastupnoi-zustrici-cim-zaversivsa-persij-samit-miru/ звернення 17.06.2024).

2. [Електронний ресурс]. Режим доступу https://uk.wikipedia.org/wiki/Договір_про_нерозповсюдження_ядерної_зброї (дата звернення 17.06.2024).

3. Черновол Є.О., Драпей С.С. Загрози ядерній безпеці України під час окупації росією об'єктів критичної енергетичної інфраструктури. Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони в умовах воєнного стану. Київ: НА СБУ. 2024. Вип. 2. С. 98–100.

4. Пономарьов В.О., Євтушенко І.В. Роль міжнародних організацій у запобіганні використання зброї масового ураження. Законодавчі аспекти протидії особливо небезпечним злочинам в Україні. Київ: Алерта, 2024. С. 325–328.

5. Пономарьов В., Вєліков С. Наслідки втрати Україною статусу ядерної держави. ІІІ Всеукраїнська конференція. Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони. Харків: ІПЮК, 2024. С. 269–270.

6. [Електронний ресурс]. Режим доступу https://khor.gov.ua/2024/06/16/36668/(дата звернення 17.06.2024).

АНАЛІЗ ОСВІТНІХ МЕТОДИК ТА ВИВЧЕННЯ ВПЛИВУ РАДІАЦІЇ НА ЗАСОБИ РАДІАЦІЙНОЇ РОЗВІДКИ В РАЙОНАХ РАДІОАКТИВНОГО ЗАБРУДНЕННЯ

Валерій КОЧКІН
співробітник СБУ

Радіаційна розвідка в зонах надзвичайної ситуації є важливим елементом забезпечення безпеки та мінімізації ризиків для людей і навколишнього середовища. Комплекс заходів, спрямованих на виявлення, ідентифікацію та оцінку рівнів радіаційного забруднення, включає дослідження конкретних районів, які піддалися впливу радіації через аварії на атомних електростанціях, радіоактивні викиди чи інші надзвичайні події.

Основними завданнями радіаційної розвідки є своєчасне виявлення радіаційних загроз, визначення їх масштабу та характеру, а також моніторинг динаміки змін радіаційного фону. Такі завдання виконуються за допомогою спеціальних технічних засобів, таких як дозиметри, спектрометри, радіометри та інші пристрої, які дозволяють точно вимірювати рівні радіації і визначати радіоактивні ізотопи, що є джерелами забруднення.

Радіаційна розвідка проводиться як у наземних, так і у повітряних умовах із використанням спеціалізованих транспортних засобів, включаючи автомобілі, гелікоптери та безпілотні літальні апарати. Використання таких засобів забезпечує охоплення великої території і дозволяє оперативно реагувати на зміни ситуації. Дані, отримані під час розвідки, використовуються для створення радіаційних карт, які відображають рівні забруднення в різних зонах, що, у свою чергу, є основою для прийняття рішень щодо евакуації, дезактивації та інших заходів реагування.

Важливим аспектом радіаційної розвідки є підготовка і навчання фахівців, які виконують ці завдання. Спеціалісти повинні володіти не тільки технічними знаннями щодо роботи з вимірювальними приладами, але й розуміти біологічні наслідки впливу радіації та дотримуватися протоколів безпеки. Їхня діяльність значною мірою визначає успішність і ефективність заходів з ліквідації наслідків радіаційних інцидентів та захисту населення.

Підготовка висококваліфікованих фахівців, здатних ефективно діяти в умовах надзвичайних ситуацій, є нагальним завданням сучасної педагогічної науки та системи освіти. Такий процес повинен ґрунтуватися на фундаментальних педагогічних засадах, що враховують як теоретичну, так і практичну складові професійної підготовки.

Одним із ключових підходів є системний підхід, який розглядає процес навчання як цілісну систему, що складається з взаємопов'язаних елементів: цілей, змісту, методів, форм організації та результатів навчання. Важливо забезпечити гармонійну інтеграцію теоретичних знань та практичних навичок, формуючи в майбутніх фахівців цілісне розуміння специфіки їхньої професійної діяльності в надзвичайних ситуаціях [1].

Важливе активне залучення здобувачів освіти до практичної діяльності, моделювання реальних ситуацій та вирішення професійних завдань. Такий підхід дозволяє розвинути необхідні практичні навички, критичне мислення та здатність приймати рішення в умовах невизначеності та стресу.

Отже, підготовка фахівців, які діятимуть в умовах надзвичайних ситуацій, вимагає комплексного підходу, який поєднує теоретичні знання та практичну підготовку на основі фундаментальних педагогічних засад. Лише за таких умов можна сформувати компетентних професіоналів, здатних ефективно діяти в екстремальних умовах та забезпечувати безпеку громадян.

Освітня методика є невід'ємною складовою педагогічної науки, що забезпечує систематизацію та впровадження теоретичних знань у практику навчання. Слід зазначити, що формування освітніх методик є циклічним процесом, який постійно еволюціонує завдяки розвитку науки, технологій та змінам у соціальному контексті. Нові наукові відкриття, трансформації в суспільстві та освітніх парадигмах вимагають перегляду та оновлення існуючих методик, а також розробки інноваційних підходів до навчання.

Етапи формування освітньої методики:

– накопичення знань про явища та процеси реального світу в різних галузях науки через наукові дослідження, експерименти та спостереження
– осмислення та систематизація знань відповідно до цілей і завдань освітнього процесу; відбір та структурування змісту навчального матеріалу;
– створення освітніх моделей, які адаптують наукові знання до рівня сприйняття здобувачів освіти з урахуванням їхніх вікових та індивідуальних особливостей;
– розробка методик, які визначають шляхи та способи ефективного засвоєння знань; вибір форм, методів і засобів навчання;
– моніторинг ефективності методик, виявлення недоліків, проблем; коригування методик через зворотного зв'язку від учасників процесу.

Отже, освітня методика трансформує знання про реальний світ в освітні моделі, що враховують цілі, зміст і специфіку навчального процесу, адже забезпечує ефективне засвоєння знань здобувачами освіти та сприяє розвитку їхніх компетентностей відповідно до потреб суспільства.

Радіаційна надзвичайна ситуація вважається однією з найбільш небезпечних та складних для реагування, оскільки пов'язана з впливом іонізуючого випромінювання, яке є невидимим та має довготривалі наслідки для здоров'я людей та навколишнього середовища. Підготовка до ефективного реагування на такі ситуації вимагає спеціальних знань та умінь від залучених фахівців [2, 3].

Крім того, необхідними є знання про організацію робіт в умовах радіоактивного забруднення, принципи розмежування зон ураження, методи дозиметричного контролю та оцінки радіаційної обстановки. Фахівці мають бути обізнані з процедурами оповіщення населення, взаємодії з іншими службами та організаціями під час ліквідації наслідків радіаційної аварії.

Важливим аспектом є психологічна підготовка персоналу, адже робота в умовах радіаційної небезпеки пов'язана з високим рівнем стресу та ризику. Необхідно навчити фахівців методам саморегуляції, підтримки психологічної стійкості та ефективної взаємодії в екстремальних ситуаціях.

Підготовка до реагування на радіаційні надзвичайні ситуації вимагає регулярних навчань та тренувань з відпрацювання практичних сценаріїв. Така практика дозволяє закріпити отримані знання, відточити навички та забезпечити злагоджену роботу всіх задіяних служб.

Отже, через високий рівень радіаційних загроз, підготовка фахівців, які будуть реагувати на них, вимагає комплексного поєднання теоретичних знань про радіацію, практичних умінь роботи з обладнанням, навичок психологічної стійкості та регулярного тренування. Лише за таких умов буде забезпечена ефективна протидія наслідкам радіаційних інцидентів та мінімізація ризиків для населення та довкілля.

Для здійснення радіаційної розвідки в зонах надзвичайної ситуації використовуються різноманітні технічні засоби. Вибір технічних засобів радіаційної розвідки залежить від конкретних завдань, умов проведення робіт, необхідної точності вимірювань та наявних ресурсів. Комплексне використання різних приладів дозволяє отримати найбільш достовірну інформацію про радіаційну обстановку в зоні надзвичайної ситуації.

Вплив радіації на технічні засоби радіаційної розвідки в зонах надзвичайної ситуації класифікують за різними критеріями [4]:

1. За характером впливу.
2. За тривалістю впливу.
3. За ступенем впливу.
4. За типом радіації.

Врахування характеру, тривалості, ступеня та типу радіаційного впливу є важливим при виборі та експлуатації технічних засобів радіаційної розвідки в зонах надзвичайної ситуації. Такий підхід дозволяє забезпечити надійність та точність вимірювань, а також безпеку персоналу, який працює з радіаційними приладами.

У педагогічному аспекті вивчення впливу радіації на технічні засоби радіаційної розвідки в зонах забруднення визначається таким чином [5]:

– предметна область;
– мета;
– завдання.

У межах даної предметної області відбувається підготовка фахівців, здатних ефективно використовувати технічні засоби радіаційної розвідки в зонах надзвичайної ситуації, забезпечувати їх надійне функціонування та приймати обґрунтовані рішення щодо застосування та захисту від радіаційного впливу.

Освітні методики вивчення впливу радіації на технічні засоби радіаційної розвідки в зонах надзвичайної ситуації класифікують за кількома критеріями [1, 2, 6]:

– за формою організації навчання;
– за методами навчання;
– за засобами навчання;
– за формою контролю знань.

Вибір відповідних освітніх методик залежить від цілей навчання, рівня підготовки здобувачів освіти, наявних ресурсів та особливостей навчального закладу. Комплексне поєднання різних форм, методів, засобів та форм контролю сприяє ефективному засвоєнню знань та формуванню практичних навичок роботи з технічними засобами радіаційної розвідки в умовах радіаційного впливу.

Вивчення впливу радіації на технічні засоби радіаційної розвідки є надзвичайно важливим аспектом підготовки фахівців, здатних ефективно діяти в умовах надзвичайних ситуацій, пов'язаних з радіаційним забрудненням. Безпосередня робота в зонах радіоактивного ураження висуває особливі вимоги до знань та практичних навичок з експлуатації радіометричного обладнання в екстремальних умовах.

З метою забезпечення належної підготовки персоналу необхідно використовувати комплексний підхід в освітньому процесі, поєднуючи різноманітні методики навчання. Включення лекційних та практичних занять, лабораторних робіт, тренінгів та симуляцій дозволяє сформувати у здобувачів освіти як ґрунтовну теоретичну базу, так і міцні практичні навички.

Використання інноваційних освітніх технологій, таких як мультимедійні презентації, комп'ютерні симуляції, натурні зразки обладнання та лабораторне устаткування, значно підвищує ефективність засвоєння матеріалу та формування компетентностей. Водночас, застосування різноманітних форм контролю знань, зокрема тестування, звітів, ситуаційних завдань та захистів проектів, дозволяє об'єктивно оцінити рівень підготовки здобувачів освіти.

Таким чином, розробка та впровадження сучасних освітніх методик вивчення впливу радіації на технічні засоби радіаційної розвідки є обов'язковою передумовою для підготовки висококваліфікованих фахівців, здатних забезпечити надійну роботу приладів в екстремальних умовах радіаційних загроз. Лише за таких умов можна гарантувати безпеку персоналу та ефективність заходів з ліквідації наслідків радіаційного забруднення.

Список використаних джерел:

1. Поліщук, О. В., Репінський, С. В., Слабкий, А.В. Формування компетенцій з безпеки життєдіяльності в студентів вищих навчальних закладів. Педагогіка безпеки. 2016. № 1(1). С. 72–80.

2. Титаренко, А.В. Методологічні засади державного управління сферою захисту населення і територій від надзвичайних ситуацій. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2016. № 1. С. 216–222.

3. Тесленко, О. Проблеми державного управління цивільним захистом щодо забезпечення контролінгу загроз та виникнення надзвичайних ситуацій у зоні відчуження. Науковий вісник: Державне управління. 2023. № 1 (13). С. 163–177. https://doi.org/10.33269/2618–0065–2023–1(13)-163–177

4. Кулаженко, А.І. Аналіз особливостей та наслідків діяльності ліквідаторів аварії на ЧАЕС в умовах радіаційної небезпеки. Вісник Національного університету оборони України. 2011. № 4. С. 161–165.

5. Барбашин, В.В. та Толкунов, І.О та Попов, І.І. Методичне забезпечення метрологічного обстеження технічних заходів радіаційного моніторингу надзвичайних ситуацій. Проблеми надзвичайних ситуацій. 2012. № 15. С. 19–25.

6. Телещак, О.А. Компетентнісний підхід як засіб підвищення рівня підготовки студентів з безпеки життєдіяльності. 2009.//[Електронний ресурс] – Режим доступу: https://ea.donntu.edu.ua/bitstream/123456789/11057/4/telechak.pdf . (дата звернення 17.06.2024)

ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ СЕКТОРУ БЕЗПЕКИ ТА ОХОРОНИ ДЛЯ ПРОТИДІЇ ПОШИРЕННЮ ТА ЗАСТОСУВАННЮ РАДІАЦІЙНОЇ, ХІМІЧНОЇ, БІОЛОГІЧНОЇ ТА ЯДЕРНОЇ ЗБРОЇ

Ірина КУЧИНСЬКА
кандидат фармацевтичних наук
співробітник СБУ

Загроза розповсюдження та застосування радіаційної, хімічної, біологічної та ядерної (далі – РХБЯ) зброї зростає в сучасному світі через розвиток технологій та політичну нестабільність. Геополітичні конфлікти та терористичні організації створюють додаткові ризики використання РХБЯ зброї, що робить питання національної безпеки вкрай актуальним. Забезпе-

чення ефективної протидії цим загрозам вимагає інтегрованого та багатоступеневого підходу, включаючи правові, технічні, освітні та міжнародні аспекти.

Під час повномасштабної війни проти України, заяви та дії росії створили серйозну загрозу безпеці ядерних та інших радіоактивних матеріалів і об'єктів в Україні, що може призвести до катастрофічних наслідків для населення та навколишнього середовища. Неодноразове застосування росією хімічних засобів боротьби з масовими заворушеннями як методу ведення війни, а також використання інших хімічних боєприпасів проти ЗСУ є грубим порушенням Конвенції про заборону хімічної зброї. Інтенсивність хімічних атак росії проти Сил безпеки України зростає, як і різноманітність хімічних боєприпасів, що використовуються. У квітні 2024 року зафіксовано 444 випадки використання російськими військами хімічних боєприпасів, що на 71 більше, ніж у березні місяці. Російські війська систематично проводять хімічні атаки, використовучи хімічну зброю для створення паніки та змушення бійців ЗСУ залишати укріплення. 2 травня Держдепартамент США звинуватив росію у використанні хлорпікрину – сльозогінного та задушливого газу. Генштаб ЗСУ заявив, що з початку вторгнення росія 815 разів використовувала хімічну зброю, з них 229 випадків у січні 2024 року [1].

Залишаються актуальними розробка та впровадження ефективної нормативно-правової бази, яка регулюватиме всі аспекти діяльності з РХБЯ матеріалами, включаючи їх виробництво, зберігання, транспортування та утилізацію; гармонізація національних законодавств з міжнародними стандартами, такими як Конвенція про заборону хімічної зброї та Договір про нерозповсюдження ядерної зброї; підвищення рівня контролю за виконанням міжнародних домовленостей через регулярні інспекції та звітність. З точки зору розвитку інфраструктури та технологій, необхідно відзначити важливість інвестування в сучасні технології для виявлення, моніторингу та нейтралізації РХБЯ загроз. Це включає розвиток систем раннього попередження та автоматизованих систем контролю, а також використання різних технологій виявлення та ідентифікації хімічного, біологічного та радіологічного забруднення. Детектори призначені для визначення наявності РХБЯ речовин, а ідентифікаційне обладнання розпізнає конкретні виявлені речовини.

Також актуальним залишається створення та удосконалення спеціалізованих лабораторій та дослідницьких центрів, що можуть оперативно реагувати на інциденти та проводити необхідні експертизи, результати яких будуть представлені в міжнародних судах. Сучасні лабораторії повинні бути оснащені новітніми приладами, здатними виявляти та аналізувати навіть найменші сліди РХБЯ матеріалів. Наприклад, для досліджень матеріалів хімічної зброї використовуються мас-спектрометри, газові та рідинні хроматографи, спектрофотометри та інші аналітичні інструменти, що дозволяють проводити високоточні аналізи. Значне місце відведено портативним приладам для експрес-аналізу на місці події, як наприклад, ручним спектрометрам та детекторам газів, які дозволяють швидко визначити наявність РХБЯ матеріалів. На підрозділи Служби безпеки України (далі – СБУ), та безпосередньо Експертну службу СБУ, покладені завдання щодо запобігання, виявлення та припинення розповсюдження і застосування зброї масового знищення. Створено експертний підрозділ, який займається техніко-криміналістичним забезпеченням контррозвідувальної, оперативно-розшукової діяльності та слідчих дій у разі використання радіоактивних, отруйно-хімічних, біологічних та ядерних речовин. Запроваджено нові судово-експертні спеціальності: дослідження радіоактивних та ядерних матеріалів, дослідження матеріалів хімічної зброї, дослідження матеріалів біологічної зброї. Наразі найбільш розвинутим напрямом в Експертній службі СБУ є проведення судових експертиз та досліджень об'єктів, пов'язаних з використанням хімічних агентів, що заборонені Міжнародною конвенцією про заборону розробки, виробництва, накопичення та застосування хімічної зброї. Задача Експертної служби СБУ, як учасника розслідувань злочинів, пов'язаних з використанням хімічної зброї, полягає у дослідженні хімічних зразків та інших об'єктів, відібраних з місця можливого застосування хімічної зброї, в рамках проведення судових експертиз, що призначаються слідчими СБУ.

Розширення науково-дослідної бази для розробки нових засобів захисту, виявлення та нейтралізації РХБЯ матеріалів, здійснюється із залученням спонсорських коштів міжнародних

організацій. Ефективна безпека щодо РХБЯ матеріалів вимагає не лише готовності до реагування, а й запобіжних заходів, розвідки та постійного обміну інформацією.

Дезактивація – це складний процес, що вимагає передових методів і знань. Використання протоколів дезактивації є критичним для виживання, оскільки недотримання дезінфекції може призвести до біологічної загрози, отруєння токсичними хімікатами тощо. Дезактивація включає механічне та хімічне видалення забруднень зі шкіри, одягу та захисного спорядження.

Хімічні загрози включають різноманітні отруйні речовини, що вимагають швидкої дезактивації. Важливо вчасно ідентифікувати ступінь хімічної загрози, визначати рівень забруднення та використовувати специфічні для кожного окремого інциденту засоби індивідуального захисту. Особливо складною є радіологічна та ядерна дезактивація через ризик радіаційного захворювання. Радіологічні загрози включають радіоактивні матеріали, які можуть швидко поширитися, а ядерні загрози – мікроскопічні частинки після вибуху або розплавлення реактора, що забруднюють довкілля. Негайного контролю потребують біологічні загрози, такі як смертельні віруси, бактерії та агенти біотероризму.

Враховуючи наявність загроз, що постійно виникають, важливими аспектом є навчання та підготовка кадрів, підвищення кваліфікації персоналу сектору безпеки та оборони шляхом проходження спеціалізованих тренінгів, навчань та участі у міжнародних програмах; створення навчальних програм у вищих навчальних закладах, що готують фахівців у сфері безпеки та захисту від РХБЯ загроз; участь у регулярних практичних заняттях та симуляціях для підготовки персоналу до можливих інцидентів з РХБЯ матеріалами.

Міжнародне співробітництво та інформаційний обмін проявляються активізацією участі у міжнародних організаціях, таких як ООН, МАГАТЕ, Організація з заборони хімічної зброї (ОЗХЗ), а також розширенням інформаційних мереж для обміну даними про потенційні загрози та інциденти з РХБЯ матеріалами. Важливими є укладання двосторонніх та багатосторонніх угод про співпрацю у сфері боротьби з тероризмом та розповсюдженням РХБЯ зброї. Спільні проекти та програми, спрямовані на забезпечення безпеки та запобігання незаконному обігу небезпечних РХБЯ матеріалів, мають велике значення для створення стабільності та безпеки України, а також для всього регіону Європейського Союзу (далі – ЄС). Прикладом є Проект № GGCPP004 «TRIGLAV», спрямований на посилення боротьби з РХБЯ загрозами на словацько-українському кордоні. Основними цілями проекту є скорочення економічних та соціальних відмінностей та зміцнення співпраці між країнами Центральної та Східної Європи, Балтії та 15 країнами ЄС. Основними завданнями проекту є зміцнення координації між правоохоронними органами країн, підвищення рівня підготовки та оснащення сил безпеки, впровадження сучасних технологій для контролю та моніторингу РХБЯ загроз, підвищення обізнаності та співпраці між владними структурами та громадськістю щодо РХБЯ загроз. Проект сприяє міжнародному співробітництву та покращенню виявлення і перехоплення незаконних РХБЯ матеріалів, підтримує навчання і підготовку кадрів у сфері РХБЯ безпеки, що підвищує обізнаність і практичні навички працівників державних установ.

Важливе місце займає підвищення рівня громадської обізнаності та участі через проведення інформаційних кампаній для підвищення обізнаності населення щодо РХБЯ загроз та способів захисту; залучення громадянського суспільства до процесів моніторингу та реагування на РХБЯ загрози через створення громадських організацій та волонтерських рухів; забезпечення доступу громадськості до інформації про державні програми та заходи, спрямовані на протидію РХБЯ загрозам.

Надзвичайний вплив небезпечних РХБЯ матеріалів становить загрозу не лише для життя і здоров'я громадян, але й має руйнівні наслідки для економічних, соціальних та екологічних інтересів суспільства. Саме тому компетентні установи повинні оперативно реагувати на виявлення незаконних РХБЯ матеріалів. Це можливо лише завдяки міжвідомчому та міжнародному співробітництву, свідомості про взаємні функції та обов'язки, застосуванню інноваційних підходів та досліджень, зокрема впровадження новітніх технологій, таких як штучний інтелект, обробка великих масивів даних, застосування дронів і робототехніки для покращення аналізу

та реагування на РХБЯ загрози, співпраця з приватним сектором для розробки та впровадження інноваційних рішень у сфері безпеки та захисту. Важливий комплексний та скоординований підхід до посилення спроможностей сектору безпеки та охорони у протидії РХБЯ загрозам, вдосконалення стратегій та механізмів захисту для забезпечення національної та міжнародної безпеки.

Список використаних джерел

1. Вісім держав відреагували на застосування хімзброї в Україні та ядерні погрози рф. URL: https://suspilne.media/762911-visim-derzav-vidreaguvali-na-zastosuvanna-himzbroi-v-ukraini-ta-aderni-pogrozi-rf/ (дата звернення 20.06.2024)

РОЛЬ І МІСЦЕ СБ УКРАЇНИ В ПРОТИДІЇ НЕЗАКОННОМУ ОБІГУ РАДІОАКТИВНИХ ТА ЯДЕРНИХ МАТЕРІАЛІВ В УМОВАХ ВОЄННОГО СТАНУ

Роман ЛЕХ
кандидат юридичних наук,
співробітник СБУ
Олег СІРИЙ
співробітник СБУ

В сучасних умовах широкомасштабної агресії рф проти України, масового порушення законів і звичаїв ведення війни з боку рф гострим питанням залишається руйнація окупантами військових об'єктів та об'єктів цивільної інфраструктури. Зухвалі дії країни-агресора призвели до захоплення стратегічного для України ядерного об'єкту критичної інфраструктури – Запорізької АЕС. рф вдалась до ядерного тероризму та шантажу як України, так і всього світу.

Загроза ядерного тероризму визнана світовою спільнотою однією з ключових проблем міжнародної безпеки. На сьогоднішній день, кількість терористичних актів постійно зростає, а відтак збільшується ймовірність використання терористами або іншими кримінальними групами чи особами у своїй діяльності радіоактивних матеріалів. Від дієвості ядерної захищеності залежить захист держави, населення та навколишнього середовища від терористичних актів, диверсій, крадіжки або будь-якого іншого протиправного діяння щодо ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання або ядерної установки (об'єкта).

В умовах збройного конфлікту на території України, постійних повітряних тривог, щоденних запусків беспілотників та крилатих ракет над атомними станціями України, ударів рф по енергетичній інфраструктурі держави, знеструмлень, пошкоджень ліній електропередач внаслідок обстрілів мали вплив на безпеку ядерних установок та завдають збитків підприємствам, діяльність яких пов'язана із поводженням з радіоактивними відходами, відпрацьованим ядерним паливом та джерелами іонізуючого випромінювання.

Найбільшою небезпекою залишається застосування окупаційними військами ядерної зброї – зброї масового ураження.

Як зазначають військові експерти, ядерні заряди можуть бути розміщені на різних типах ракет, бомбах та артилерійських снарядах, якими країна-агресор постійно обстрілює територію України.

Зрозуміти, що під час ракетного обстрілу була використана ядерна зброя тактичного рівня, можна тільки після вибуху та при наявності даних про радіоактивне забруднення території. Факторами ураження при використанні ядерної зброї є ударна хвиля, світлове випромінювання, іонізуюче випромінювання та радіоактивне забруднення. Радіологічний розсіюючий пристрій, або «брудна бом-

ба», є, фактично, вибухівкою з радіоактивним матеріалом. Під час детонації радіоактивні речовини розпорошуються в довкіллі вибуховою хвилею та призводять до радіоактивного забруднення певної території та об'єктів, **які** на ній знаходяться. Через обмежений радіус дії «брудна бомба» може використовуватися росією для залякування мирного населення на територіях, віддалених від лінії фронту. Важливо, що досі у світі не *було* задокументовано реальних випадків підривів радіологічних розсіюючих пристроїв, тож, поки їх можна вважати інструментом інформаційно-психологічного впливу.

Відповідно до п.п. 2 п. 1 статті 19 Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII Служба безпеки України входить до складу сектору безпеки і оборони та, як державний орган спеціального призначення з правоохоронними функціями, забезпечує державну безпеку у сфері боротьби з тероризмом.

Відповідно до ч. 2 статті 2 Закону України «Про Службу безпеки України» від 25.03.1992 № 2229-XII (далі – Закон), до завдань СБ України входить попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України та, відповідно п. 3 статті 24 Закону, здійснювати розслідування кримінальних правопорушень, віднесених законодавством до компетенції СБ України.

Крім того, відповідно до п. 17 статті 24 Закону СБ України у ході виконання своїх основних завдань зобов'язана брати участь у розробленні та здійсненні заходів щодо фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання.

Таким чином, на виконання норм вищезазначеного Закону службова діяльність органів СБ України спрямована на:

– запобіганні – організації відповідних заходів з контролю та захисту ядерних матеріалів та установок від зловмисних та протиправних дій;
– виявленні – вжиттю заходів з розкриття (в рамках компетенції СБУ) протиправних дій стосовно ядерних та інших радіоактивних матеріалів, а також пов'язаних з ними установок та іншої інфраструктури;
– реагуванні – організації відповідних заходів з ефективного реагування на випадки зловмисних та протиправних дій, включаючи аналіз та встановлення походження вилучених матеріалів і речовин.

Підсумовуючи, необхідно зазначити, що до безпосередніх заходів, спрямованих на забезпечення ядерної безпеки на національному рівні, належить фізичний захист, який має забезпечувати захищеність ядерних матеріалів та установок, а також інших джерел іонізуючого випромінювання з метою недопущення вчинення несанкціонованих дій, а також облік і контроль ядерних та радіоактивних матеріалів.

Всі вище перелічені чинники об'єднують заходи, спрямовані на недопущення використання ядерного матеріалу в військових цілях та потрапляння ядерного та радіоактивного матеріалу в незаконний обіг.

Від дієвості заходів ядерної безпеки залежить ступінь ризиків для держави, пов'язаних із незаконним обігом ядерних та інших радіоактивних матеріалів, а також із терористичними актами.

Особливої небезпеки набуває ситуація, пов'язана з незаконним обігом радіоактивних та ядерних матеріалів, у тому числі які знаходились на тимчасово окупованих територіях Донецької, Луганської, Запорізької та Херсонської областей.

Слід зазначити, що в умовах військової агресії протиправні дії, пов'язані з незаконним обігом радіоактивних та ядерних матеріалів, можуть бути здійснені в результаті:

– пошкодження та розграбування підприємств і установ, де використовуються радіоактивні та ядерні матеріали, радіонуклідні джерела іонізуючого випромінювання (металургійні заводи, центри ядерної медицини, видобувні підприємства, медичні та наукові установи тощо);

– виникнення аварій на атомних електростанціях та руйнування енергоблоків в наслідок ворожих обстрілів;
– намірів застосування ядерної зброї або «брудної» бомби.

Відповідно до компетенції Служби безпеки України (стаття 216 «Підслідність» Кримінально-процесуального кодексу України від 13.04.2012 № 4651-VI), слідчі органи безпеки здійснюють досудове розслідування кримінальних правопорушень, передбачених статтєю 265–1 «Незаконне виготовлення ядерного вибухового пристрою чи пристрою, що розсіює радіоактивний матеріал або випромінює радіацію» Кримінального кодексу України (далі – КК України) від 05.04.2001 № 2341-III.

Слід зазначити, що норми, які передбачають відповідальність за злочини у сфері незаконного обігу радіоактивних матеріалів, передбачені статтями: 261 КК України «Напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення», 262 КК України «Викрадення, привласнення, вимагання вогнепальної зброї, бойових припасів, вибухових речовин чи радіоактивних матеріалів або заволодіння ними шляхом шахрайства або зловживання службовим становищем», 265 КК України «Незаконне поводження з радіоактивними матеріалами», 265 КК України «Незаконне поводження з радіоактивними матеріалами», 266 КК України «Погроза вчинити викрадання або використати радіоактивні матеріали»,267^1 КК України «Порушення вимог режиму радіаційної безпеки», 274 КК України «Порушення правил ядерної або радіаційної безпеки».

Вищезазначені статті Кримінально-процесуального кодексу України відносяться до компетенції Національної поліції України.

Підводячи підсумки, можна зазначити, що роль і місце СБ України в протидії незаконному обігу радіоактивних та ядерних матеріалів, впершу чергу, пов'язана із взаємодією з представниками сектору безпеки і оборони (зокрема, підрозділів з радіаційного, хімічного та біологічного захисту Збройних Сил України, Національної гвардії та Державної прикордонної служби), в частині погодження спільних алгоритмів дій і механізмів оперативного реагування на ядерні загрози з боку росії, комплексному відпрацювання заходів з виявлення незаконного перебування небезпечних радіоактивних матеріалів на території України, здійснення перевірочних заходів в місцях масового перебування людей та на об'єктах критичної інфраструктури, а також транспортних засобах, які диверсанти рф можуть потенційно використовувати для перевезення радіоактивних матеріалів для створення «брудної» бомби, моніторингу блокпостів у прифронтових і деокупованих районах, пунктів пропуску через кордон тощо.

Список використаних джерел:

1. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII.
2. Закон України «Про Службу безпеки України» від 25.03.1992 № 2229-XII.
3. Кримінальний кодекс України від 05.04.2001 № 2341-III.
4. Кримінально-процесуальний кодекс України від 13.04.2012 № 4651-VI.

ПРОГРАМНЕ ПРОГНОЗУВАННЯ ХІМІЧНОЇ ОБСТАНОВКИ ПРИ НАДЗВИЧАЙНИХ СИТУАЦІЯХ, ЯКІ ВИНИКЛИ ВНАСЛІДОК ВИКОРИСТАННЯ ХІМІЧНОЇ ЗБРОЇ

Андрій МЕЛЬНИЧЕНКО
доктор філософії,
старший викладач кафедри організації
та технічного забезпечення аварійно-рятувальних робіт
Національного університету цивільного захисту України
Максим КУСТОВ
доктор технічних наук, професор,
начальник наукового відділу з проблем
цивільного захисту та техногенно-екологічної
безпеки Національного університету
цивільного захисту України
Олексій БАСМАНОВ
доктор технічних наук, професор,
головний науковий співробітник наукового
відділу з проблем цивільного захисту та
техногенно-екологічної безпеки Національного
університету цивільного захисту України

Надзвичайні ситуації (НС) з викидом небезпечних хімічних речовин (НХР), що виникли внаслідок використання хімічної зброї, характеризуються значними розмірами зони ураження, яка може досягати декількох квадратних кілометрів. Додатковим ускладненням є знаходження в зоні ураження великої кількості цивільного населення та необхідність залучення значних сил та засобів на ліквідацію наслідків такої НС [1]. Це становить значну загрозу для населення, території та навколишнього середовища, які є основними об'єктами системи цивільного захисту. З метою забезпечення екологічної безпеки в зоні атмосферного забруднення з викидом небезпечних газів та прийняття управлінського рішення по евакуації населення важливим є проведення коректного моніторингу та точного прогнозування розвитку надзвичайної ситуації [2]. Прогнозування розвитку надзвичайної ситуації є обов'язковим етапом для прийняття коректного управлінського рішення по ліквідації наслідків застосування хімічної зброї. Особливо суттєвим процес прогнозування є при виникненні НС з викидом газоподібних небезпечних хімічних речовин.

Для забезпечення достатньої точності розрахунку розмірів зон хімічного забруднення необхідне врахування значної кількості факторів, які умовно можна розподілити на два блоки – метеорологічні умови та параметри викиду. До метеорологічних умов відносяться напрямок та швидкість вітру, температура та вологість повітря, атмосферний тиск. До параметрів викиду відносяться вид хімічної речовини, її температура, густина та тиск, інтенсивність викиду. Існуючі методи та засоби запобігання надзвичайним ситуаціям з викидом небезпечних речовин в атмосферному повітрі здатні впливати на зону ураження на висотах декілька метрів.

Ліквідація наслідків надзвичайних ситуацій (НС), які характеризуються викидом в атмосферне повітря шкідливих та радіоактивних речовин, є надзвичайно складним завданням, що вимагає застосування спеціалізованих методів та технологій. Одним з найбільш поширених підходів у світі є використання рідинних завіс, які утворюються за допомогою наземної аварійно-рятувальної техніки. Рідинні завіси використовуються для осадження шкідливих та радіоактивних речовин з атмосфери шляхом розпилення дрібнодисперсного потоку води. Цей метод дозволяє знизити концентрацію забруднювачів у повітрі, що полегшує роботу аварійно-рятувальних служб

і служб контролю екологічної безпеки. Основними аспектами цього методу є інтенсивність потоку рідини, площа осадження та хімічна реакція рідини з небезпечними речовинами.

Надзвичайні ситуації, що виникають внаслідок використання хімічної зброї, мають свої унікальні особливості. Однією з головних характеристик таких ситуацій є потужні вражаючі фактори та висока швидкість поширення небезпечних хімічних речовин (НХР). Це вимагає швидкого реагування з боку служб, які займаються ліквідацією наслідків НС. Основні заходи включають швидку евакуацію працівників, службовців та населення з зони ураження, постійний моніторинг концентрацій НХР в повітрі та оцінку масштабів забруднення, деконтамінацію територій, будівель та обладнання від НХР, забезпечення медичної допомоги постраждалим, а також надання психологічної підтримки населенню.

Застосування рідинних завіс і загальна ліквідація наслідків НС супроводжуються численними труднощами. Служби контролю екологічної безпеки та аварійно-рятувальні підрозділи стикаються з викликами, такими як координація дій між різними службами, наявність і підтримка в робочому стані необхідної техніки та обладнання, підготовка персоналу до роботи в умовах НС, проведення регулярних тренувань і навчань, а також постійне оновлення і вдосконалення методів оцінки ризиків та розробка нових підходів до ліквідації наслідків НС. У цілому, ліквідація наслідків надзвичайних ситуацій, пов'язаних з викидом шкідливих та радіоактивних речовин, вимагає комплексного підходу, що включає використання сучасних технологій, ефективну координацію дій та постійну готовність до роботи в умовах підвищеної небезпеки.

У зв'язку з цим особливо важливим стає спрощення та підвищення швидкості прогнозування хімічної обстановки при надзвичайних ситуаціях, що виникли внаслідок використання хімічної зброї. Враховуючи всі зазначені виклики, вирішення цього питання є актуальним і необхідним.

Для ефективного прогнозування хімічної обстановки при НС з викидом небезпечних газів внаслідок використання хімічної зброї була розроблена методика, яка базується на математичній моделі. Ця методика реалізована у вигляді програмного продукту «Прогноз НХР» (рис. 1). Даний програмний продукт дозволяє швидко і точно моделювати хімічну обстановку, що значно полегшує роботу аварійно-рятувальних підрозділів.

Рис. 1. Інтерфейс програмного комплексу «Прогноз НХР»

Інтерфейс програмної реалізації методики прогнозування наслідків надзвичайних ситуацій з викидом небезпечних газів умовно розділений на декілька робочих областей. Найбільшу частину займає інтерактивна карта місцевості, інтегрована із сервісом Google Maps. Це дозволяє оперативно шукати координати епіцентру викиду або навпаки за відомими координатами відображати епіцентр на карті. Координати епіцентру викиду заносяться в окрему область у правій верхній частині інтерфейсу.

Окремим блоком інтерфейсу є блок «Атмосфера» в яку вносяться найбільш значущі метеорологічні параметри атмосфери, такі як температура, тиск, швидкість та напрямок вітру. Ці параметри легко можна отримати із портативної метеостанції або від офіційних представників Державного Гідрометеоцентру.

В окремий блок виведені параметри викиду. З бібліотеки найбільш розповсюджених небезпечних газів оператор може обрати необхідний та занести величину інтенсивності викиду цього газу із технологічного апарату.

Останній блок інтерфейсу призначений для введення параметрів осадження хмари небезпечного газу, а саме ширину зони осадження, інтенсивність та дисперсність водяного потоку, відстань від осередку викиду до початку зони осадження.

Методика працює наступним чином:

1. По прибуттю до місця НС керівник ліквідації надзвичайної ситуації визначає місце викиду та встановлює його у програмному комплексі «Прогноз НХР» за допомогою інтерактивної карти або координат;
2. Керівник ліквідації надзвичайної ситуації під час проведення розвідки місця НС спеціального маркування та візуального контролю визначає вид небезпечного газу та оцінює інтенсивність його викиду. Ці данні заносяться до програмного комплексу «Прогноз НХР»;
3. Співробітники штабу за допомогою портативної метеостанції, яка є штатним обладнанням на автомобілях радіаційного та хімічного захисту визначають основні метеорологічні параметри та вносять їх до блоку «Атмосфера» запропонованого програмного комплексу. У випадку відсутності портативної метеостанції, співробітники штабу зв'язуються із оперативним черговим регіонального відділу Державної Гідрометеослужби та дізнаються від нього необхідні данні. В цьому випадку отриманні данні будуть менш точними, так як вони виміряні на найближчому пункті спостереження, а не безпосередньо в зоні НС;
4. Керівник ліквідації НС проводить оцінку доступних сил та засобів для проведення осадження небезпечної хмари та при наявності відповідних ресурсів розставляє рятувальників із розпилюючи ми стволами для осадження хмари.
5. Виходячи із кількості розпилюючи стволів та їх тактико-технічних характеристик керівник ліквідації надзвичайної ситуації або відповідальна особа із його штабу визначає параметри осадження та заносить у відповідний блок інтерфейсу програмного комплексу;
6. Після натискання на кнопку «Розрахунок» програмний комплекс автоматично проводить прогнозування та наносить результати на карту;
7. Керівник ліквідації надзвичайної ситуації проводить оцінку результатів прогнозування та приймає управлінське рішення щодо зміни позиції рятувальників, збільшення або зменшення кількості стволів, що подано на осадження та про необхідність проведення евакуації із прилеглих територій.

Таким чином, розроблено програмна реалізація та запропоновано алгоритм роботи з нею, що дозволить використовувати розроблену методику прогнозування наслідків надзвичайних ситуацій із викидом небезпечних газів внаслідок використання хімічної зброї, практичним працівникам оперативно-рятувальних підрозділів без окремих навичок програмування. Програма «Прогноз НХР» містить блоки «Атмосфера», «Викид», «Осадження» для введення вхідних параметрів та інтерактивну карту місцевості для виведення результатів прогнозування на неї.

Список використаних джерел:

1. Oggero A., Darbra R.M., Munoz M., Planas E., Casal J. A survey of accidents occurring during the transport of hazardous substances by road and rail. Journal of hazardous materials. 2006. № 133(1–3). P. 1–7.

2. Pospelov B., Rybka E., Meleshchenko R., Borodych P., Gornostal S. Development of the method for rapid detection of hazardous atmospheric pollution of cities with the help of recurrence measures. Eastern-European Journal of Enterprise. 2019. № 1/10 (97). P. 29–35.

ОРГАНІЗАЦІЯ ПРОТИДІЇ ЗАГРОЗАМ ВІД ЗБРОЇ МАСОВОГО УРАЖЕННЯ

Віктор ПОНОМАРЬОВ
доктор філософії,
доцент Національного юридичного
Університету імені Ярослава Мудрого

Використання зброї масового ураження (ЗМУ) в сучасних конфліктах є надзвичайно небезпечним і має серйозні глобальні наслідки [1]. Міжнародне співтовариство, включаючи багатосторонню конвенцію про заборону хімічної зброї [2], активно працює над договорами та угодами, щоб обмежити поширення та використання цих видів зброї і забезпечити захист населення та навколишнього середовища.

Наявність великої кількості ЗМУ у країни-агресора дає їй можливість робити злочини проти людства без побоювань про покарання, принаймні у найближчі часи.

Спільнота міжнародних організацій та країн працює над спробами запобігти таким випадкам та покарати винних. У цьому інформаційному ключі виникає питання про дійсні можливості міжнародних організацій щодо допомоги у запобіганні військової агресії. Організації, такі як Організація Об'єднаних Націй (ООН), Європейський Союз (ЄС), НАТО та інші зазвичай відіграють важливу роль в цьому процесі.

Важливо зазначити, що реакція міжнародних організацій та країн на військову агресію залежить від конкретної ситуації, політичних обставин та правових рамок. Спільна дія та співпраця багатьох країн можуть допомогти запобігти військовій агресії та зміцнити світовий устрій.

Нажаль, після відмови від ядерної зброї у 1996 році Україна залишилась беззахисною проти агресора, який, на підставі Будапештського меморандуму був одним з гарантів недоторканості українських територій [3]. І тільки інші фігуранти Будапештської угоди (США та Великобританія) намагаються фінансово та матеріально надавати допомогу у війні проти росії. Крім того, західні партнери занепокоєні можливими наслідками застосування противником ЗМУ, на підставі чого організовуються заходи по підготовці фахівців щодо реагування на дані загрози.

Для забезпечення безпеки населення та військових сил є дуже доцільним поширення та розвиток навчальних програм по захисту від засобів ураження ЗМУ. Це обумовлюється важливістю наступних складових [1]:

1. Навчання людей основам захисту від ЗМУ є ключовим для забезпечення їхньої безпеки. Обізнаність громадян щодо, способів виявлення або розпізнавання та захисту від потенційно небезпечних речовин, можуть сприяти уникненню ситуацій, що становлять загрозу їхньому здоров'ю та життю.

2. Добре підготовлені військовослужбовці, володіючи знаннями про захист від ЗМУ, можуть ефективно впоратися з потенційними загрозами під час участі військових операціях або в ході врегулювання збройних конфліктів.

3. Поширення навчальних програм по захисту від ЗМУ допомагає забезпечити громадську безпеку. Якщо більше людей знатимуть як реагувати на ситуації, пов'язані з хімічною зброєю, то це допоможе локалізувати та мінімізувати поширення небезпеки.

4. Поширення навчальних програм сприяє підготовці фахівців відповідної кваліфікації, які зможуть працювати у сфері розробки, випробування та застосування засобів захисту від ЗМУ. Це розширює можливості подальшого дослідження та інновацій в цій галузі.

Здібності силового сектору та оборони України з питань протидії загрозі ЗМУ базуються на розвитку та модернізації військових структур, навчання кадрів, співпраці з міжнародними організаціями та партнерами, а також впровадженні стратегічних планів та технологій. Україна активно співпрацює з партнерами з метою зміцнення своєї обороноздатності та забезпечення безпеки нації.

Протидія загрозам від ЗМУ включає в себе ряд заходів, таких як міжнародні угоди на заборону розповсюдження такої зброї, співпрацю між країнами у сфері роззброєння, розвиток технологій для виявлення та нейтралізації загроз, а також підвищення свідомості населення про потенційні ризики. Окрім того, важливо вдосконалювати систему реагування на випадки використання зброї масового ураження, а також забезпечити ефективний контроль над її зберіганням і застосуванням.

Протистояння загрозам від ЗМУ є дуже важливим завданням сучасного світу. Організація ООН відіграє ключову роль у цьому питанні, сприяючи міжнародній співпраці та контролю над поширенням таких видів зброї. Крім того, багато країн мають свої власні програми та агентства, спрямовані на запобігання поширенню та застосуванню ЗМУ, а також розробку відповідних стратегій безпеки. У зв'язку з цим, співпраця між країнами та обмін інформацією є критично важливою для успішного запобігання таким загрозам [4].

Список використаних джерел:

1. Пономарьов В.О., Євтушенко І.В. Роль міжнародних організацій у запобіганні використання зброї масового ураження. Законодавчі аспекти протидії особливо небезпечним злочинам в Україні. Київ: Алерта, 2024. С. 325–328.

2. Конвенція про заборону розробки, виробництва, накопичення, застосування хімічної зброї та про її знищення. Ратифіковано Законом України N187-XIV (187–14) від 16.10.98. URL: https://zakon.rada.gov.ua/laws/show/995_182#Text (дата звернення: 14.06.2024).

3. Пономарьов В., Вєліков С. Наслідки втрати Україною статусу ядерної держави. ІІІ Всеукраїнська конференція. Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони. Харків: ІПЮК, 2024. С. 269–270.

4. Міжнародна програма запобігання розповсюдженню зброї масового ураження (ICP). URL: https://ua.usembassy.gov/uk/embassy-uk/kyiv-uk/sections-offices-uk/defense-threat-reduction-office-uk/international-counterproliferation-program-icp/ (дата звернення: 14.06.2024).

ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ В КОНТЕКСТІ РОЗБУДОВИ ЄДИНОЇ СИСТЕМИ ПРОТИДІЇ CBRN ЗАГРОЗАМ

Віктор ХЛАНЬ
кандидат технічних наук, старший науковий співробітник
співробітник СБУ
Віталій ОНІЩЕНКО
співробітник СБУ

Відповідно до ст. 216 КПК України до компетенції слідчих органів безпеки віднесено здійснення досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку, передбачених ст. 439 «Застосування зброї масового знищення», ст. 440 «Розроблення, виробництво, придбання, зберігання, збут, транспортування зброї масового знищен-

ня», ст. 265–1 «Незаконне виготовлення ядерного вибухового пристрою чи пристрою, що розсіює радіоактивний матеріал або випромінює радіацію», ст. 201 «Контрабанда» (контрабанда отруйних, сильнодіючих, вибухових речовин, радіоактивних матеріалів, зброї або боєприпасів), ст. 333 «Порушення порядку здійснення міжнародних передач товарів, що підлягають державному експортному контролю» КК України [1].

Водночас, Служба безпеки України є головним органом у загальнодержавній системі боротьби з терористичною діяльністю, який у межах своєї компетенції здійснює боротьбу з тероризмом шляхом проведення оперативно-розшукових та контррозвідувальних заходів, спрямованих на запобігання, виявлення та припинення терористичної діяльності, здійснює досудове розслідування злочинів, пов'язаних з терористичною діяльністю (ст. 4 і 5 Закону України «Про боротьбу з тероризмом») [2].

Останнім часом тероризм набуває загрозливого характеру, цьому сприяють, зокрема, агресивні дії російської федерації, яка ракетами фізично знищує частини українських міст, подальше загострення ситуації на Близькому Сході, посилення інтересу до України з боку міжнародної організованої злочинності у сферах незаконної міграції, легалізації (відмивання) доходів, одержаних злочинним шляхом, контрабанди зброї, небезпечних матеріалів та наркотичних засобів, відходів біологічних, хімічних, радіаційних речовин, ядерних матеріалів.

При цьому міжнародна практика свідчить, що велику небезпеку становить можливість застосування терористами матеріалів, які є компонентами для створення зброї масового ураження – ядерної, хімічної, біологічної.

Таким чином виникає нагальна потреба підвищення можливостей системи виявлення, контролю та боротьби з проявами тероризму в умовах поширення асиметричних загроз, пов'язаних із можливим використанням терористичними групами та організаціями біологічних, хімічних, радіаційних речовин, ядерних матеріалів як компонентів зброї масового знищення.

Положення національної антитерористичної системи значною мірою визначається міжнародною антитерористичною системою, яка містить в собі найбільш вдалий досвід боротьби з тероризмом у різних країнах світу. Зважаючи на загрозу тероризму з використанням зброї масового знищення одним із основних критеріїв національної антитерористичної системи слід визнати її здатність адаптуватися до міжнародних антитерористичних структур і заходів, а також оперативно переймати світовий досвід та в найкоротші строки втілювати в практичну діяльність національних антитерористичних підрозділів.

Продовжуючи дослідження можна зазначити, що сьогодні у світовому безпековому середовищі досить уживаними стали абревіатура та словосполучення: CBRN risks, CBRN incident, CBRN agents, CBRN materials, CBRN policy, CBRN information, CBRN structure тощо. CBRN (Chemical, Biological, Radiological, and Nuclear) загрози є однією з найбільших проблем для міжнародної безпеки [3–7]. Як зазначалося вище, використання компонентів зброї масового знищення може мати катастрофічні наслідки для людства, включаючи масові втрати серед населення, тривалу шкоду навколишньому середовищу та глобальну дестабілізацію. Внаслідок цього міжнародна спільнота створила різноманітні організації, ініціативи та альянси для попередження, підготовки та реагування на такі загрози, серед них:

Організація з заборони хімічної зброї (OPCW), здійснює контроль за виконанням Конвенції про заборону хімічної зброї, інспекції об'єктів, знищення запасів хімічної зброї, розслідування випадків використання хімічної зброї. До структури входять: Генеральна конференція, Виконавча рада, Технічний секретаріат. Серед найбільш суттєвих проектів: Інспекція та знищення хімічної зброї в Сирії; підтримка та підготовка кадрів для країн-учасниць, включаючи Україну, щодо безпечного зберігання та ліквідації хімічних матеріалів [8].

Міжнародне агентство з атомної енергії (МАГАТЕ), сприяє мирному використанню ядерної енергії, попереджує її використання у військових цілях, проводить інспекцію ядерних об'єктів, забезпечує ядерну безпеку, надає технічну допомогу. Основними структурними елементами є: Генеральна конференція, Рада керівників, Секретаріат. Проєкти – програма з забезпечення ядерної безпеки в Україні, технічна підтримка та вдосконалення систем безпеки українських атомних електростанцій [9].

Ініціатива з глобального партнерства проти розповсюдження зброї масового знищення (GPP), до сфери відповідальності відноситься: запобігання поширенню зброї масового знищення, знищення запасів CBRN матеріалів, підготовка кадрів, розмінування. До складу входять визначені країни-учасниці, робочі групи, координаційний офіс. Проєкти – знищення запасів хімічної зброї в Лівії; проекти з підвищення безпеки та охорони радіологічних матеріалів в Україні [10].

Програма НАТО з забезпечення CBRN безпеки, працює над підвищенням готовності та реагування на CBRN загрози серед країн-членів НАТО, розробляє стандарти, спільні навчання, здійснює обмін відповідною інформацією. Складається з країн-члени, відповідних груп з питань CBRN захисту та визначених робочих груп. Проєкти – проведення спільних навчань з українськими військовими підрозділами, надання обладнання для детекції та захисту від CBRN загроз [11].

Європейський Союз CBRN центри передового досвіду (EU CBRN CoE), забезпечує підвищення міжнародної співпраці та координації у сфері CBRN безпеки, розробляє спільні програми, організовує та надає технічну підтримку, проводить підготовку спеціалістів, сприяє обміну відповідною інформацією. Містить регіональні секретаріати, національні контактні пункти та робочі групи. Проєкти – в рамках співпраці з Україною організовано підготовку фахівців у сфері CBRN безпеки, розроблено та впроваджено окремі складові системи моніторингу та контролю CBRN загроз [12].

Програма США з забезпечення CBRN безпеки (US CBRN Defense Program), спрямована на підвищення готовності та реагування на CBRN загрози для США та їх союзників, в рамках програми розробляються та впроваджуються новітні технології детекції та захисту, здійснюється підготовка військових та цивільних кадрів, організовується співпраця з міжнародними партнерами. Складається із спеціалізованих підрозділів, дослідницьких центрів Міністерства оборони США. Проєкти – підтримка України через навчання українських спеціалістів використанню обладнання для виявлення та захисту від CBRN загроз, надання технічної допомоги та відповідного обладнання [13].

Як показано вище, існує багато міжнародних організацій, ініціатив та альянсів основою метою яких є попередження, підготовка та реагування на CBRN загрози. Так ми маємо складне питання та ряд проблемних ситуацій, які пов'язані з нагальною потребою в інтеграції до наведених вище міжнародних структур та подальшим забезпеченням на державному рівні ефективної роботи органів, служб та підрозділів до сфери компетенції яких відноситься попередження, виявлення, протидія проявам тероризму в умовах поширення асиметричних загроз, пов'язаних із можливим використанням терористичними групами та організаціями біологічних, хімічних, радіаційних речовин, ядерних матеріалів як компонентів зброї масового знищення.

В контексті зазначеного маємо певну кількість проблем серед них: складність координації дій між різними організаціями та країнами, що знижує ефективність глобальної відповіді на CBRN загрози; недостатнє фінансування ініціатив та програм з CBRN безпеки; прискорення темпів розвитку науково-технічного прогресу та в наслідок цього спрощення доступу до подвійних технологій, які можуть бути використані як для мирних, так і для військових цілей, насамперед CBRN компоненти; існування прогалин в міжнародному праві щодо контролю за CBRN матеріалами тощо.

Серед можливих шляхів вирішення вказаних проблем пропонується: створення інтегрованих платформ для обміну інформацією, розробка та імплементація спільних стратегій реагування; залучення додаткових фінансових ресурсів через міжнародні гранти та програми співпраці; регулярне оновлення нормативно-правової бази за напрямом інвестицій в військові дослідження та розробки; ратифікація та імплементація нових міжнародних договорів, посилення контролю за виконанням існуючих угод; створення спеціалізованих координаційних центрів на національному та міжнародному рівнях для управління проектами з CBRN безпеки.

При цьому окрему увагу зосередимо: по-перше, на потребі включення проектів з CBRN безпеки у національні та міжнародні програми розвитку. Це дозволить забезпечити фінансування,

технічну підтримку та залучення необхідних ресурсів. По-друге, на розробці науково-обґрунтованих критеріїв та стандартів для реалізації проектів з CBRN безпеки. Це включає в себе проведення досліджень для визначення оптимальних методів та підходів, розробку стандартів якості, безпеки та ефективності. По-третє, розробці програм підготовки та навчання кадрів для реалізації проектів з CBRN безпеки. Це включає в себе навчальні курси, тренінги та практичні заняття, використовуючи при цьому наукові методи для оцінки ефективності навчання та внесення коректівів у програми.

Підводячи підсумок можна зазначити, що посилення спроможностей сектору безпеки та оборони в контексті розбудови єдиної системи протидії CBRN загрозам передбачає здійснення конкретних кроків. Серед яких, як варіант, імплементація передових міжнародних практик та формування відповідного національного плану дій спрямованого на розбудову єдиної системи протидії CBRN загрозам. Цей план має враховувати специфічні умови та потреби нашої країни, зокрема з урахуванням збройної агресії з боку росії. При цьому основні кроки у формуванні такого плану мають передбачати:

- аналіз загроз та потреб України: проведення комплексного аналізу потенційних CBRN загроз та оцінка наявних ресурсів і здатностей для адекватної протидії.
- розробку стратегії протидії: визначення конкретних заходів та заходів, необхідних для забезпечення безпеки нації від CBRN загроз.
- створення координаційних механізмів: формування спеціальних організацій/комітетів, які відповідатимуть за координацію дій у сфері протидії CBRN загрозам та впровадження плану дій.
- залучення міжнародної підтримки: встановлення механізмів співпраці з міжнародними партнерами та організаціями для обміну досвідом та технічної підтримки.
- навчання та підготовку кадрів: здійснення навчань, тренінгів та симуляцій для підготовки фахівців із сфери CBRN безпеки.
- моніторинг та оцінку: встановлення системи моніторингу та оцінки результатів впровадження плану дій для постійного аналізу ефективності та внесення необхідних коректівів.

В цілому, реалізація такого плану дій сприятиме підвищенню рівня безпеки та готовності сектору безпеки та оборони України до відповіді на CBRN загрози, забезпечуючи при цьому необхідну координацію, якісне ресурсне забезпечення, а також відповідну підготовку кадрів.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. URL: https://zakon.rada.gov.ua/ laws/show/4651–17#Text. (дата звернення 17.06.2024).

2. Закон України «Про боротьбу з тероризмом». URL: https://zakon.rada.gov.ua/ laws/show/638–15#Text. (дата звернення 17.06.2024).

3. Зменшення хімічних, біологічних, радіологічних і ядерних ризиків. URL: https://cbrn-risk-mitigation.network.europa.eu/index_en. (дата звернення 17.06.2024).

4. Project on Minimum Standards and Non-Binding Guidelines for First Responders Regarding Planning, Training, Procedure and Equipment for Chemical, Biological, Radiological and Nuclear (CBRN) Incidents. URL: https://www.nato.int/ nato_static_fl2014/assets/pdf/pdf_2016_08/20160802_140801-cep-first-responders-CBRN-eng.pdf (дата звернення 17.06.2024).

5. Policy on chemical, biological, radioactive and nuclear threats and attacks. URL: https://policy.un.org/sites/policy.un.org/files/files/documents/2020/Oct/spm_chapter_iv_section_q_-_cbrn_policy_1.pdf. (дата звернення 17.06.2024).

6. Управління ХБРЯ безпекою. URL: https://unicri.it/index.php/topics/cbrn/security_governance. (дата звернення 17.06.2024).

7. CBRN TERRORISM INSURANCE: A RISK TOO FAR? URL: https://www.insurancethoughtleadership.com/commercial-lines/cbrn-terrorism-insurance-risk-too-far (дата звернення 17.06.2024).

8. Organisation for the Prohibition of Chemical Weapons. URL: https://www.opcw.org. (дата звернення 17.06.2024).

9. IAEA. URL: https://www.iaea.org/. (дата звернення 17.06.2024).

10. Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (the Global Partnership. URL: https://www.gpwmd.com/. (дата звернення 17.06.2024).

11. Chemical, Biological, Radiological and Nuclear (CBRN). URL: https://www.nato.int/cps/uk/natohq/news_217722.htm?selectedLocale=en. (дата звернення 17.06.2024).

12. European Union (EU) Chemical, Biological, Radiological and Nuclear (CBRN) Risk Mitigation Centres of Excellence (CoE). URL: https://cbrn-risk-mitigation.network.europa.eu/eu-cbrn-centres-excellence_en. (дата звернення 17.06.2024).

13. Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO-CBRND). URL: https://www.usa.gov/agencies/joint-program-executive-office-for-chemical-biological-radiological-and-nuclear-defense. (дата звернення 17.06.2024).

ДЕЯКІ ПОГЛЯДИ НА СТАН ПРОБЛЕМИ ЗАХИСТУ ВІЙСЬК ВІД ЯДЕРНОЇ ЗБРОЇ ЯК ЗБРОЇ МАСОВОГО УРАЖЕННЯ

Ігорь ЧЕРНЯВСЬКИЙ
кандидат технічних наук, доцент,
професор кафедри РХБ захисту
Військового інституту танкових військ
Національного технічного університету
«Харківський політехнічний інститут»
Олександр КОРНІЙЧУК
співробітник СБУ

Глибоке занепокоєння світової спільноти з приводу навчань нестратегічних ядерних сил рф, відновлення робіт зі створення ядерної зброї на нових фізичних принципах ядерними державами [1–4], змушує переглядати концептуальні підходи до управління ризиками в умовах ядерної загрози.

І справа тут не у визначеннях – зброя масового знищення або масового ураження (ЗМУ). У будь якому випадку факт застосування або надмалих тактичних ядерних боєприпасів, або великої потужності є недопустимою подією для людства. Але для силових структур сектора безпеки та оборони це виклик на зрілість та готовність ефективно використовувати заходи захисту, які добре відомі з минулого століття.

До 1994 року для Збройних сил України (ЗСУ), захист військ від ядерної зброї (ЯЗ) був частиною загального комплексу заходів захисту від ЗМУ і мав на меті не допустити ураження військ та об'єктів тилу ЯЗ або максимально послабити результати його впливу і тим самим зберегти боєздатність військ та забезпечити успішне виконання тих задач, що стоять перед ними. Необхідно відмітити, що у цих умовах, першочерговим завданням є виявлення та оцінка обстановки, що склалася, яка під час прогнозування базується на інформації від засобів засічки параметрів ядерних вибухів (ЯВ). Ієрархічна структура постів спостереження, розрахунково-аналітичних груп (станцій, центрів) усіх силових відомств складали єдину систему виявлення та оцінювання наслідків (ЕСВОН) застосування ЗМУ.

З відмовою нашої держави від ЯЗ і взагалі від ЗМУ, що формально привело до зміни назви хімічних військ на війська РХБ захисту, неформальною стороною став перехід від хімічного (хіміко-технічного) забезпечення бойових дій та частин, як виду бойового (оператив-

ного) забезпечення, до забезпечення радіаційного, хімічного, біологічного захисту (РХБз), де місця для технічних засобів засічки ЯВ вже не було. «Реформування» найважливішого, завдання «Засічка параметрів ЯВ» як рудименту холодної війни, відбувалося у вигляді скорочення радіотехнічних полків (комплекс К-191-Р**)** та світлотехнічних батальйонів засічки (К-611(612)).

Необхідно відмітити, що договір про всеосяжну заборону ядерних випробувань (ДВЗЯВ) заборонив усі форми ядерних випробувань в рамках спроб роззброєння та відмови від ЯЗ, але разом з цим виникли старі проблеми, наприклад, як гарантувати, що учасники не порушать умов договору. З цією метою було створено Міжнародну систему моніторингу (IMS), що включає 321 станцію спеціального контролю (ССК), у тому числі і на території України [4–9] (як правило сейсмічні). Але основна відмінність систем засічки ЯВ на випадок ядерної війни від систем контролю ядерних випробувань у мирний час (ССК) полягає в необхідності високої оперативності отримання інформації про ЯВ та високої часової роздільної здатності. Крім того, існує проблема і нижньої межі реєстрації тротилового еквіваленту ЯВ (1 кт), що безумовно стимулювало розвиток тактичної ядерної зброї у ядерних країнах. Інша проблема – ідентифікація типу застосованого ядерного боєприпасу (атомний, термоядерний або нейтронний), від якого залежить перерозподіл виділяємої енергії між уражаючими факторами ЯВ.

Проблема стає ще більше актуальною для ЗСУ у сучасних умовах, якщо розуміти, що таке завдання як «Оцінка ядерної обстановки», яка є першопричиною виникнення складної пожежної, інженерної, радіаційної, медичної обстановки у осередку ядерного ураження – достовірно здійснюється тільки за наявністю оперативної інформації від технічних засобів засічки параметрів ЯВ, які у армійській ланці відсутні. Розробка нових технічних рішень з питань виявлення та оцінювання ядерної обстановки після застосування ЯЗ припинилася з кінця 90-х років минулого століття. Значна доля досліджень у той час була присвячена радіаційній обстановці в результаті ліквідації наслідків аварії на ЧАЕС. Спроба переорієнтувати заходи захисту ЗМУ до забезпечення РХБз, (потім до просто РХБ захисту) та до інших видів бойового (оперативного) забезпечення (інженерного, медичного та інші) призвело до втрати акцентів з цих питань, втрати системного підходу до ефективного реагування на ці загрози (за залишковим принципом витрати ресурсів), що в кінцевому рахунку призвело до втрати такого виду бойового (оперативного) забезпечення як захист від ЗМУ.

Необхідно відмітити, що вказані заходи, повинні були виконувати усі підрозділи (не тільки «фахівці хімічних військ») незалежно від того, чи є загроза або вона малоймовірна. Крім того, на зорі забезпечення РХБ захисту існувало таке поняття, як – штатні та позаштатні підрозділи РХБ захисту (спостерігачі, розвідники). Найбільш важкі завдання в інтересах окремих структурних підрозділів виконували фахівці військ РХБз. Але с переходом на стандарти НАТО дані питання теж залишаються відкритими.

З прийняттям доктрини з ХБРЯ за стандартами НАТО знову виникає завдання оцінювання ядерної обстановки. В центрі уваги передових країн світу довгий час були проблеми ядерного тероризму, радіологічної (брудної) бомби, і відповідно майже не приділялася увага проблемам виявлення та оцінювання наслідків можливого застосування тактичної ЯЗ. Але як показує аналіз відкритих джерел, розробки у даній галузі не зупинялися.

Основним завданням, у цих умовах, для науковців усіх рівнів, на наш погляд, є реанімація спеціальності: 20.02.23 – засоби захисту від ЗМУ, яка нажаль не заявлена ні одною спеціалізованою вченою радою України.

Список використаних джерел:

1. Теленко О.М. Ядерна зброя як чинник міждержавних відносин в Південній Азії. Актуальні проблеми міжнародних відносин. Київ, 2015. Вип. 124 (ч. ІІ). С. 22–29.

2. Spence D’Anne E. Zero Nuclear Weapons and Nuclear Security Enterprise Modernization. Strategic Studies Quarterly. 2011. Vol. 5, No 3. P. 121–133.

3. Wachs L. The Role of Nuclear Weapons in Russia's Strategic Deterrence. Implications for European security and nuclear arms control. SWP Comment. 2022. 68. 7 Seiten. doi:10.18449/2022C68.

4. Kristensen H.M., Korda M., Reynolds E. Russian nuclear weapons. Bulletin of the Atomic Scientists. 2023. Vol. 79(3). P. 174–199. DOI: https://doi.org/10.1080/00963402.2023.2202542 .

5. Куліков С.П., Андрощук Р.А., Андрущенко Ю.А., Корнієнко В.І. Можливість використання інформації Головного центру спеціального контролю для визначення місцеположення та оцінювання масштабів техногенних катастроф. Збірник наукових праць. Вип. 9 / Житомирський військовий інститут імені С.П. Корольова Державного університету телекомунікацій. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: – Житомир: ЖВІ ДУТ, 2014.– С. 156–163.

6. Мережа геофізичних спостережень ГЦСК як інформаційний сегмент системи моніторингу надзвичайних ситуацій/ Р.А. Андрощук, О.І Солонець, І.В. Толчонов, Ю.О. Гордієнко// Системи управління, навігації та зв'язку: зб. наук. праць.– Х.: ХУПС, 2011.– Вип.218. С. 281–283.

7. Моніторинг сейсмічними засобами потенційних джерел надзвичайних подій/ Р.А. Андрощук, Ю.О. Гордієнко, В.А. Кирилюк. О.І Солонець// Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. Наук. праць.– Житомир: ЖВІ НАУ, 2011.– Вип.5 –С.173–180.

8. Анрющенко Ю.А. Спосіб ідентифікації природи сейсмічних джерел на основі спектрально-часового аналізу коливань/ Р.А. Андрощук, Ю.О. Гордієнко//Геофизический журнал.– 2009.– Т. 31.– № 6.– С. 140–146.

9. Теорія побудови систем географізичного моніторингу: навч. Посіб. /Р.А. Андрощук, О.І. Рибачук. В.В. Стрінда та ін.– Житомир: РУТА. 2012.– 220 с.

ОРГАНІЗАЦІЯ ВЗАЄМОДІЇ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ ТА СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ У РЕАГУВАННІ НА РХБЯ-ІНЦИДЕНТИ

Юрій ЧЕЧІЛЬ
доктор філософії у галузі права,
співробітник СБУ
Вікторія БІЛА
доктор юридичних наук, доцент,
співробітник СБУ

В умовах збройної агресії проти України достатньо гостро постає питання про організацію належної взаємодії між органами публічної адміністрації та сектором безпеки і оборони у питаннях реагування на можливі радіаційні, хімічні, біологічні, ядерні (далі – РХБЯ) інциденти, а також організації безпечного документування фактів застосування зброї масового знищення (далі – ЗМЗ), у разі настання такої події на території України.

Варто вказати, що на сьогодні в Україні наявна низка формалізованих процедур реагування на радіаційні інциденти [1–3], формування яких відбувалось в умовах мирного часу, без урахування викликів та загроз, зумовлених веденням активних бойових дій на території України. Крім того, Спільна заява держав-учасниць Ініціативи з обміну інформацією у сфері РХБЯ безпеки та захищеності щодо України щодо неодноразового застосування країною-агресором хімічних засобів боротьби з масовими заворушеннями як методу ведення війни, а також зростання інтенсивності хімічних атак проти сил безпеки та сил оборони України (далі – Спільна заява) [4] додатково актуалізувала питання розробки планів реагування на хімічні інциденти.

З цього питання у літературі зазначається про необхідність забезпечення високого рівня координації між національними агентствами за для ефективного реагування на РХБЯ інциденти. Світова спільнота визначає подальший розвиток міжвідомчої взаємодії у галузі РХБЯ головним пріоритетом глобальної безпеки [5].

Питання організації взаємодії між органами публічної адміністрації, сектором безпеки та оборони, прокуратурою у реагуванні на можливі РХБЯ-інциденти має не лише два контексти (мирного та воєнного часу), однак і структурні та функціональні виміри. Структурний рівень полягає в організації міжвідомчої взаємодії на центральному та територіальному рівнях, а також внутрішньовідомчої взаємодії в середині державних органів. Функціональний вимір визначає порядок взаємодії за видами діяльності під час реагування на РХБЯ-інциденти, як-то деконтамінація, надання медичної допомоги постраждалим, відбір зразків РХБЯ-матеріалів та направлення їх на дослідження, забезпечення «chain of custody», проведення аварійно-рятувальних, відновлювальних робіт тощо.

Зарубіжний досвід містить низку прикладів такого системного підходу до розбудови національних спроможностей міжвідомчої взаємодії у реагуванні на можливі РХБЯ інциденти. Зокрема йдеться про рамкові документи із запобігання, захисту, зменшення негативних наслідків, реагування та відновлення після надзвичайних подій, зокрема й РХБЯ інцидентів, що розроблені і діють у Сполучених Штатах Америки (далі – США) [6]. Зазначені документи є підставою для розробки федеральних міжвідомчих оперативних планів [6], серед яких саме Оперативний план реагування та відновлення (далі – План) [7] міститиме деталізовані додатки щодо реагування на різні види інцидентів. У додатках розкриваються фази інциденту та заходи з реагування, визначаються державні органи, що беруть участь у реагуванні на інцидент, їх ролі, обов'язки та спроможності, можливості залучення недержавних інституцій тощо. Крім того, у додатках здійснено опис функцій та складу «тимчасових» утворень, що можуть бути створені для реагування на інцидент. Так, наприклад, для реагування на ядерний/радіаційний інцидент можуть бути скликані: Оперативна група (Task Force) з ядерних/радіологічних інцидентів, Стратегічна група зі зброї масового знищення (далі – WMDSG), Єдина координаційна група тощо. Ці групи не є постійно діючими й скликаються у разі настання певної події. Одна і та сама група може скликатись для реагування на різні типи надзвичайних подій. Так, WMDSG скликається у разі реальної загрози застосування ЗМЗ та складається із представників різних державних агенцій під керівництвом ФБР.

У додатках до Плану обов'язково визначаються випадки залучення правоохоронних органів, а також їх функції, повноваження та порядок координації діяльності.

Так, згідно з додатком 4 «Операції реагування та запобігання умисним нефтяним/хімічним інцидентам» до Плану кожен хімічний інцидент розглядається як вчинений умисно, допоки не буде встановлено зворотного. «Умисний» хімічний інцидент передбачає залучення ФБР, що координуватиме діяльність правоохоронних органів, а також розслідування інциденту та розвідувальну діяльність відносно цього [8, с. 47].

На національному рівні утворюється WMDSG під управлінням ФБР, що здійснює міжвідомчу координацію реагування на інцидент на стратегічному рівні. Частиною WMDSG є Група координації ліквідації наслідків (далі – CMCU), яку очолює Федеральне управління з надзвичайних ситуацій (далі – FEMA).

Для діяльності на місці інциденту утворюється Об'єднаний центр операцій (далі – JOC), що є командним пунктом через який ФБР координує діяльність правоохоронних органів, розслідування, збір даних і контртерористичні заходи. JOC очолює керівник інциденту від ФБР (on-scene commander). Керівник інциденту також відповідає за зв'язок із WMDSG.

До JOC включено декілька груп:

Командна група, що складається з повноважних приймати рішення вищих посадових осіб федеральних та регіональних агентств і відомств, а також недержавних суб'єктів. До основних завдань командної групи віднесено управління інцидентом (від реагування до відновлення), обмін інформацією про інцидент, координація антитерористичних операцій та операцій із лік-

відації наслідків, схвалення використання ресурсів правоохоронних органів;

Оперативна група, що здійснює збір доказів та розслідування інциденту. До її складу окрім оперативних та слідчих працівників, також включаються криміналісти.

Група підтримки операцій, що забезпечує логістику, зв'язок, комунікацію з громадськістю, роботу зі свідками та постраждали особами.

Група з управління наслідками, що складається з представників регіональних управлінь FEMA, приватних суб'єктів та інших органів публічної адміністрації і здійснює аварійно-рятувальні та відновлювальні роботи.

Вибір ФБР як головного органу в координації заходів з реагування на хімічний інцидент обґрунтовується тим, що місце хімічного інциденту розглядається як місце вчинення злочину. Від так збереження та збір доказів має вирішальне значення для встановлення винних осіб та отримання додаткової інформації про інші можливі інциденти, диверсії тощо [8, с. 49].

Питання збереження та належного збору доказів особливо актуалізується при подальшому призначенні судових експертиз в межах кримінального провадження. Адже можливості якісного аналізу в межах експертної спеціальності, наприклад, дослідження матеріалів хімічної зброї, безпосередньо залежить від кількості, якості та часу відібрання зразків, пакування тощо. Від так, залучення фахівця, який зможе надати консультативну допомогу на місці інциденту щодо зазначених питань може значно полегшити процес розслідування РХБЯ інциденту.

У підсумку варто зазначити, що можливість імплементації практик взаємодії публічної адміністрації та сектору безпеки і оборони США в систему реагування на можливі РХБЯ інциденти в Україні є питанням, що повинне бути обговорено у фахових колах. Однак, на сьогодні цілком очевидною є необхідність сприйняття декількох основних положень, а саме: посилення міжвідомчої взаємодії з одночасним визначенням сфер відповідальності кожного залученого до реагування суб'єкта; забезпечення належного документування можливого РХБЯ-інциденту, в тому числі відбору зразків та подальшого проведення судових експертиз; посилення ролі судової експертизи та криміналістики у реагуванні на можливі РХБЯ-інциденти.

Зважаючи на важливість належного поводження з вилученими на місці можливого РХБЯ інциденту доказами, зокрема й забезпечення простежуваності їх руху з моменту вилучення на місці події, на внутрішньовідомчому рівні усіх залучених державних органів варто вжити заходів щодо: визначення вимог до компетенції співробітників, які залучатимуться до роботи на місцях можливих РХБЯ-інцидентів; розробки та затвердження тактик, технологій та процедур відбору, пакування та направлення на експертизу зразків, відібраних на місцях РХБЯ-інцидентів; відпрацювання практичних навичок взаємодії із особами (криміналістами, судовими експертами), що залучатимуться до реагування на можливі РХБЯ інциденти в якості спеціалістів.

Список використаних джерел:

1. Порядок взаємодії органів виконавчої влади та юридичних осіб, які провадять діяльність у сфері використання ядерної енергії, в разі виявлення радіоактивних матеріалів у незаконному обігу: постанова Кабінету Міністрів України від 2 червня 2003 р. № 813. URL: https://zakon.rada.gov.ua/laws/show/813–2003-%D0%BF#Text. (дата звернення 20.06.2024).

2. Державний план взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними: постанова Кабінету Міністрів України від 24 липня 2013 р. № 598. URL: https://zakon.rada.gov.ua/laws/show/598–2013-%D0%BF#Text. (дата звернення 20.06.2024).

3. План реагування на радіаційні аварії: Наказ Державного комітету ядерного регулювання України та Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 17.05.2004 № 87/211. URL: https://zakon.rada.gov.ua/laws/show/z0720–04#Text.

4. Спільна заява держав-учасниць Ініціативи з обміну інформацією у сфері радіаційної, хімічної, біологічної та ядерної (РХБЯ) безпеки та захищеності щодо України, травень 2024 року, м. Прага, Чеська Республіка. URL: https://mfa.gov.ua/news/spilna-zayava-derzhav-uchasnic-iniciativi-z-obminu-informaciyeyu-u-sferi-rhbya-bezpeki-ta-zahishchenosti-shchodo-ukrayini. (дата звернення 20.06.2024).

5. Benolli, F., Guidotti, M., Bisogni, F. (2021). The CBRN Threat. Perspective of an Interagency Response. In: Jacobs, G., Suojanen, I., Horton, K., Bayerl, P. (eds) International Security Management. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978–3–030–42523–4_29.

6. National Planning Frameworks. URL: https://www.fema.gov/emergency-managers/national-preparedness/frameworks

7. Response and Recovery Federal Interagency Operational Plan First Edition March 2023. https://www.fema.gov/sites/default/files/documents/fema_response-recovery-fiop.pdf. (дата звернення 20.06.2024).

8. Oil and Chemical Incident Annex to the Response and Recovery Federal Interagency Operational Plans February 2021. URL: https://www.fema.gov/sites/default/files/documents/fema_incident-annex-oil-chemical.pdf. (дата звернення 20.06.2024).

Секція 4
ОСОБЛИВО НЕБЕЗПЕЧНІ ПОСЯГАННЯ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ: СУЧАСНІ УМОВИ, РОЗСЛІДУВАННЯ, ПРОТИДІЯ

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ КОНВЕРГЕНЦІЇ ВПЛИВУ НА ЦІЛЬОВІ АУДИТОРІЇ: ОНЛАЙН-ІГРИ, СОЦІАЛЬНІ МЕРЕЖІ ТА МЕДІА-ПРОСТІР

Сергій БАЗАРНИЙ
Національний університет оборони України

Актуальність теми – інформаційної безпеки держави набула критичного значення в умовах сучасних гібридних загроз [1–2], зокрема в контексті широкомасштабної збройної агресії російської федерації проти Україні. Конвергенція [3] цифрових платформ створює нові виклики для забезпечення інформаційної безпеки, оскільки різні цільові аудиторії можуть бути використані для здійснення впливів та маніпуляцій в межах проведення інформаційних (психологічних) операцій.

Окреслимо конвергенцію впливу на цільові аудиторії основні з яких можна виділити наступні:

1. Гравці комп'ютерних онлайн-ігор [4];
2. Користувачі (далі агенти) соціальних мереж;
3. Споживачі інформації через Медіа-простір.

Розглянемо окремо кожну з вищезазначених цільових аудиторій.

1. Гравці комп'ютерних онлайн-ігор:
– використання онлайн-ігор як сучасної платформи для протидії пропаганді та дезінформації [5];
– великий, за обсягом, людський потенціал для вербування та радикалізації через геймерські спільноти;
– необхідність у розробці та застосуванні спеціальних алгоритмів та методів моніторингу для аналізу контенту в онлайн-іграх.

2. Агенти Соціальних мереж [6]:
– поширення фейкових новин та маніпулятивної інформації через соціальні платформи;
– вплив на громадську думку та політичні настрої населення через таргетовану рекламу і ботоферми;
– роль використання соціальних мереж у проведенні інформаційних кампаній щодо мобілізації населення та координації дій під час бойових дій (зіткнень), тощо.

3. Споживачі інформації через Медіа-простір:
– проблеми контролю та перевірки достовірності інформації у традиційних та нових медіа;
– стратегічна комунікація та контрпропаганда як засоби протидії дезінформації;
– взаємодія державних органів з медіа для забезпечення єдності інформаційного простору.

До основних механізмів удосконалення інформаційної безпеки можна визначити наступні інтегровані підходи:

– розробка комплексних стратегій, що включають моніторинг, аналіз та оперативне реагування на сучасні виклики та загрози;
– впровадження міжвідомчої співпраці для обміну інформацією та координації дій між різними державними та недержавними структурами.

Технологічними рішеннями можуть бути наступні дії:
– використання можливостей штучного інтелекту та машинного навчання для виявлення та нейтралізації дезінформаційних кампаній, психологічних акцій, тощо;
– розробка та впровадження ефективних заходів кіберзахисту на основі сучасних цифрових та інформаційно-комунікаційних технологій.

Законодавчі ініціативи:
– удосконалення законодавства в сфері інформаційної безпеки з урахуванням сучасних викликів;
– врегулювання діяльності агентів соціальних мереж, розробників та гравців онлайн-ігор для запобігання поширенню шкідливого контенту.

Освітні програми та підвищення обізнаності:
– розроблення та впровадження актуальних навчальних програм для інформування населення щодо критичного мислення та розпізнавання дезінформації.
– інформаційні кампанії для підвищення рівня кібергігієни серед різних цільових аудиторій.

До практичних рекомендацій можна запропонувати наступне:
– створення спеціалізованих центрів:
– заснування центрів інформаційної безпеки для моніторингу, аналізу та реагування на інформаційні загрози, які повинні мати чітко визначену структуру, завдання та повноваження для ефективної роботи.

Партнерство з приватним сектором:
– співпраця з технологічними компаніями для розробки інноваційних рішень у сфері інформаційної безпеки;
– впровадження механізмів саморегуляції в соціальних мережах та онлайн-іграх для запобігання розповсюдженню шкідливого контенту.

Під час проведення моніторингу та аналізу інформаційного простору:
– створення системи постійного моніторингу інформаційного простору для швидкого виявлення та нейтралізації дезінформації;
– використання аналітичних інструментів для прогнозування та попередження інформаційних атак.

Перспективами розвитку інноваційних технологій можна вважати наступне:
– розробка та впровадження новітніх технологій для захисту інформаційного простору, таких як блокчейн для забезпечення прозорості та довіри до інформації;
– використання технологій доповненої реальності та віртуальної реальності для створення безпечного та контрольованого медіа-простору.

Розширення інфраструктури забезпечення кібербезпеки:
– розвиток національної інфраструктури забезпечення кібербезпеки з урахуванням сучасних викликів і загроз;
– інвестування в дослідження та розробки для забезпечення конкурентоспроможності та стійкості країни.

Міжнародна співпраця:
– важливість міжнародної співпраці в боротьбі з інформаційними загрозами, зокрема обмін досвідом та найкращими практиками з іншими країнами;
– участь у міжнародних організаціях та ініціативах для координації дій та вироблення спільних стратегій протидії дезінформації та кіберзагрозам.

Отже, забезпечення належного рівня інформаційної безпеки держави в умовах конвергенції впливу потребує комплексного та системного підходу. Такий підхід повинен інтегрувати сучасні

технологічні інновації, спрямовані на підвищення обізнаності громадян та розвиток критичного мислення, а також активну міжнародну співпрацю та партнерство. Лише консолідовані та скоординовані зусилля держави, інституцій громадянського суспільства та приватного сектору (бізнесу) на національному та глобальному рівнях сприятимуть формуванню стійкому та надійному захисту інформаційній екосистемі, яка є життєво необхідною для протидії дезінформації, інформаційним (психологічним) операціям, кібервпливам та іншим заходам з боку противника.

Список використаних джерел:

1. Указ Президента України № 685/2021 від 15 жовтня 2021 року Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки» URL: https://www.president.gov.ua/documents/6852021–41069. (дата звернення 10.06.24р.).

2. Указ Президента України № 447/2021 від 26 серпня 2021 року Стратегія кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 10.06.24р.).

3. Є. Цимбаленко. Конвергенція мас-медіа і медіа комунікацій. Український науковий журнал «ОСВІТА РЕГІОНУ». Університет «Україна»Всеукраїнська асоціація політичних наук (ВАПН). URL: https://social-science.uu.edu.ua/article/1043. (дата звернення 10.06.24р.).

4. J. Clement, Feb. 29, 24 Online gaming – Statistics and Factc. URL: https://www.statista.com/topics/1551/online-gaming/#topicOverview. (дата звернення 10.06.24р.).

5. Закон України «Про боротьбу з тероризмом» від 20.03.2003, № 638-IV URL: https://ips.ligazakon.net/document/T030638?an=198. (дата звернення 10.06.24р.).

6. Nasery, M., Turel, O., & Yuan, Y. (in press). Combating Fake News on Social Media: A Framework, Review, and Future Opportunities. Communications of the Association for Information Systems, 53, pp-pp. Retrieved from URL: https://aisel.aisnet.org/cais/vol53/iss1/9. (дата звернення 10.06.24р.).

СВІТОГЛЯДНЕ ПРОТИСТОЯННЯ – ЯК ОСНОВА ІНФОРМАЦІЙНОЇ БОРОТЬБИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Олександр БАЛАНДА
провідний науковий співробітник
ЦВСД Національного університету оборони України

Протягом всієї історії людства світоглядна концепція змінювалась і розвивалась. Від зародження цивілізації і до сьогодення, питання війни та миру вважалися складовою частиною людського світогляду. Своєрідні погляди на війну та мир, їхню роль у житті людства багато в чому сформували Історичні типи світогляду – міфологічний, релігійний, науково-філософський.

У часи домінування міфологічного світогляду війна вважалася нормою, а не винятком. Боги війни були центральними фігурами будь-якого язичницького пантеону. Світоглядні концепції війни відображали духовні, політичні та економічні реалії того часу. Легітимності війні в очах людей надавало оголошене через жерців схвалення богів. Питання справедливості війни вирішувалося через її релігійний характер і тому раціональних сумнівів не викликало.

Релігійний тип світогляду змінив характерну для античності концепцію і започаткував нову – концепцію священної війни. Згідно з нею, війна може бути справедливою тільки в тому випадку, якщо вона була започаткована з моральних мотивів.

Формування науково-філософського погляду на світ призвело до формування таких світоглядних ідей як міжнародне гуманітарне право та правове регулювання справедливості війни. З'явилася ідея про те, що війна має стати крайнім засобом розв'язання конфліктів. Виникає теорія «гарячої війни» і «холодної війни».

Світоглядне протиборство у сучасних умовах ґрунтується на принципах, що обмежують жорстокість війни та захищають права цивільного населення. Однією з основних концепцій у світоглядному протиборстві в умовах збройної агресії є ідея про протистояння тоталітарного фаталізму та демократичного детермінізму. Ця концепція ґрунтується на ідеї відповідальності суспільства, держави та кожного згідно норм гуманітарного міжнародного права та звичаїв і законів війни, які регулюють поведінку сторін у конфліктах і захищають права мирного населення.

У сучасних війнах також важливу роль відіграє технологічний прогрес. Інформаційне середовище стало глобальним явищем, яке здійснює максимальний вплив на світоглядні установки сторін будь-якого конфлікту. Принципова різниця між світоглядом громадян країни-агресора та світоглядом громадян країни – жертви агресії полягає у тому, що суспільство, держава та громадяни країни-агресора змушені постійно шукати виправдання власним агресивним діям. На цей внутрішній діалог впливає пропаганда країни-агресора. Це вимагає від розробки все нових стратегій та тактик ведення інформаційної війни, а також врахування можливих наслідків таких дій.

Особливо актуально це у війнах, де немає чіткої лінії між військовими та цивільними об'єктами, а також у війнах, з використанням таких методів, як тероризм, що можуть ставити під загрозу життя та безпеку мирного населення. У цілому, світоглядне протиборство у сучасних війнах є складовою інформаційного протиборства та зосереджується на розумінні складної природи конфліктів та вимагає нового підходу до ведення бойових дій, захисту прав людини та захисту цивільного населення.

Отже, у сучасній війні світоглядне протистояння залишається актуальною темою. Сучасні погляди на це явище базуються на ідеї мирного врегулювання конфліктів та захисту прав людини. Однак світоглядна спроба виправдати агресію відкидає людство до міфологічного типу світогляду, який розглядає війну як неминучий атрибут людської природи, що обумовлюється бажанням досягнути перемоги та підкорити чужу територію і народ. Релігійний світогляд формував погляд на війну як виконання Божої волі та захист віри. Науково-філософський тип світогляду розглядає війну, як засіб реалізації ідеологічних та економічних інтересів нації.

Список використаних джерел:

1. Арон, Реймон. Мир і війна між націями. Пер. з фр. Віктор Шовкун, Зоя Борисюк та Григорій Філіпчук. Київ: «Юніверс», 2000.

2. Bhugra, Dinesh. The Global Prevalence of Schizophrenia. PLoS Med. 2005 May; 2(5): e151. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1140960/16. (дата звернення 16.06.24р.)

ВИКОРИСТАННЯ СЕРЕДОВИЩА СОЦІАЛЬНО-ОРІЄНТОВАНИХ РЕСУРСІВ У ІНФОРМАЦІЙНОМУ ПРОТИБОРСТВІ

Євгеній БЄЛЯЄВ
асистент Національного юридичного
університету імені Ярослава Мудрого

Поняття інформаційне суспільство міцно увійшло в систему координат сучасного світу. Незавойовані території збереглися тільки в інформаційній сфері, а тому пошук нових комунікативних можливостей, розвиток маніпулятивних технік і сугестивних технологій прямо пов'язані зі спробами глобального впливу на окремі мережеві співтовариства й покоління загалом [1, с. 111].

За даними аналітичного звіту креативної агенції We Are Social [3] на початок 2024 року в Україні було 29,64 мільйона користувачів Інтернету. Користувачів соціальних мереж – 24,3 мільйо-

на, що дорівнювало 64,9 відсотка загального населення. Водночас дані, опубліковані в інструментах рекламного планування провідних соціальних медіаплатформ, свідчать про те, що на початок 2024 року в Україні соціальними мережами користувалися 21,18 мільйона користувачів віком від 18 років. Загалом 82 відсотка загальної бази користувачів Інтернету в Україні (незалежно від віку) використовували принаймні одну платформу соціальних мереж на початку 2024 року.

Рекламні ресурси (інструменти) провідних компаній, які володіють соціальними мережами надають наступну інформацію про кількість користувачів в Україні (на початок 2024р.): Facebook – 13,85 млн; Facebook Messenger – 8,60 млн; YouTube – 24,30 млн; Instagram – 12,40 млн; TikTok – 16,47 млн; LinkedIn – 5,10 млн; X (Twitter) – 4,55 млн.

Вищевказана статистика користувачів охоплює людей віком від 18 років. Але, можна сказати, що повною мірою розкриває масштаб користувачів у країні.

Відсутність цензури, висока періодичність публікацій і різний формат передачі інформації у соціальних мережах, створюють сприятливе інформаційне середовище для побудови колективних ідентичностей, створення образів «своїх» і «чужих» спільнот. Окрім того, за рахунок інтеграції ЗМІ та посадових осіб у соціальні мережі, останні в Україні стали ще і задовольняти потреби своїх користувачів в інформації.

Варто додати, що ще однією характерною рисою цього соціального середовища є присутність штучної комунікації, що здійснюється фейковими структурами, інтернет-ботами, клонами авторитетних лідерів, організацій, які значно ускладнюють пошук потрібної інформації, обмін думками й маніпулюють громадськими настроями всередині спільнот [4, с. 274–275].

Широкі можливості і перспективи використання соціальних мереж не залишилися поза увагою військово-політичного керівництва, фахівців інформаційно-психологічного протиборства, розвідувальних служб провідних країн світу. На сьогодні соціальні мережі досить активно використовуються для просування власних інтересів, для введення в суспільний обіг тенденційної та відверто шкідливої для суспільства інформації, а також для організації і керівництва соціальними заворушеннями.

«Архітектура» соціальних мереж характеризується відкритістю, гнучкістю, простотою користування та доступністю. Це в свою чергу сприяє спроможності громадян швидко консолідуватися та організовуватися, без будь-якого управління центрального органу.

Основними динамічними характеристиками соціальних мереж як загальнодоступного інформаційного ресурсу для впливу на суспільну думку, є:

– транскордонність середовища обміну інформацією та дій і юрисдикцій мережних операторів;
– інтеграція в єдиний цифровий інформаційний ресурс мобільних, комп'ютерних, теле- і радіомереж;
– появу професійних «інтернет-революціонерів», «експертів», що використовують інформаційний ресурс для підготовки, організації та проведення «кольорових революцій», здійснення інформаційних акцій чи інформаційно-психологічних спеціальних операцій.

Маніпулювання інформацією у кіберпросторі, з метою зміни або впливу на її семантичну природу, називається семантичною атакою. Даний вид маніпуляцій можна характеризувати як психологічний вплив, метою якого є впровадження в психіку адресату цілей, намірів чи бажань, установок, які не збігаються з тими, які у нього є на даний момент. Тобто семантичні атаки використовують особливості соціальних мереж та людської психології для проведення дезінформаційних кампаній, вони здатні змінити поведінку цільових груп населення.

Існує такий вид семантичних атак, як астротурфінг – штучне формування громадської думки з використанням безлічі фальшивих або анонімних акаунтів у соцмережах. Керують такими акаунтами програми-боти або проплачені інтернет-тролі («ляльки зі шкарпетки», як їх ще називають на Заході).

Термін «астротурфінг» походить від назви американської компанії AstroTurf, що виробляє штучне покриття для стадіонів, яке імітує траву так само як сфабрикована громадська ініціатива імітує справжню.

Проведене дослідження соціальних мереж [6] Центром передового досвіду у галузі стратегічних комунікацій НАТО, у вересні-жовтні 2022 року, показало, що фейкові облікові записи використовуються для популяризації різноманітної непов'язаної інформації. Завданнями такої популяризації були:

– підвищення видимості впливових людей і знаменитостей в Інтернеті;
– реклама криптовалютних проектів та шахрайських проектів;
– поширення порнографічний контенту;
– рекламування послуг з маніпулювання соціальними медіа;
– просування інформації, пов'язаної з різними російськими політиками; рекламування політичних матеріалів.

Повномасштабне вторгнення російської федерації в Україну також залишило свій відбиток і на ринку маніпуляцій у соціальних мережах. Фейкові облікові записи використовуються для поширення прокремлівських наративів, таких як «біологічні лабораторії США в Україні», «США та НАТО вторглися в Афганістан, Лівію, Ірак, В'єтнам тощо», а також для заперечення звірств, скоєних російською армією. У TikTok спостерігається використання фальшивих залучень для посилення дописів російських блогерів, які просувають кремлівський порядок денний і мобілізують підтримку для війни проти України. Значна кількість зареєстрованих у соціальних мережах осіб залучається російськими спецслужбами для вербування українців до агентурної мережі та організації каналів збору інформації про пересування техніки й особового складу Збройних Сил України, що здійснюють оборону держави.

Слід не забувати, що інформаційний вплив з боку третіх країни, часто може бути ненормальним або навіть ворожим, а саме:

– вводити в оману – приховування інформації та мети, з якою вона поширюється;
– проводиться з метою розколу суспільства;
– порушення природніх процесів в суспільстві – втручання в роботу інститутів, найпоширенішим прикладом чого є втручання у вибори.

Самі інформаційні кампанії спираються на три основні стратегії:

– позитивна стратегія – створення зв'язного наративу для обраної аудиторії, такий наратив відповідає вже наявним загальноприйнятим нормам суспільства і лише доповнює їх;
– негативна або підривна стратегія – перешкоджає виникненню конструктивного наративу, а також прагне знищити вже наявні;
– стратегія відволікання – переключає увагу аудиторії з небажаних тем на будь-які інші з метою максимально ускладнити сприйняття і змусити людей відмовитися від оцінки того, що відбувається.

На сьогодні негативні зміни в інформаційному полі можуть трансформуватися в «культуру скасування». Подібна форма бойкоту відома людству ще з давніх часів, раніше вона називалася остракізмом – практикою політичної боротьби у деяких полісах Стародавньої Греції, коли людину, що могла загрожувати демократії, виганяли з міста.

Досить швидко практики «культури скасування» поширилися на сферу політики. Такому розвитку сприяло те, що політики, політичні інститути, партії та рухи активно використовують соціальні мережі для просування своїх ідей, поширення інформації про свою діяльність та прямого спілкування.

«Культуру скасування» частіше розглядають як інструмент економічної та політичної боротьби. Особливість даної «культури» можна розглядати як феномен соціальних мереж, що, створює умови для когнітивної вразливості, особливо у сфері політики. Соціальні мережі формують «хибні зони компетентності» і стають інструментом «кольорових революцій», оскільки «масова людина» сприймає складну реальність як просту та зрозумілу, і демонструє готовність включитися в активне просування запропонованого їй ззовні розуміння «єдино правильного». У політиці та міжнародних відносинах «культура скасування» перетворюється «на зброю політичного контролю» і служить засобом «для солідаризації решти».

Нерідко ініціатори використання «культури скасування» діють для мобілізації суспільства через соціальні мережі, щоб залучити найбільшу кількість прихильників та надати максимальний вплив на окремих людей, компанії чи формальні інститути влади. Для мобілізації використовуються конкретні випадки несправедливості або порушення норм, навколо яких формується певний дискурс, що призводить до поляризації думок та суспільної мобілізації. Дослідники зазначають, що «культура скасування» може бути інструментом нечесної конкуренції чи навіть маргінальних політичних гравців. Вони також вказують, що вона є виявом «масової людини» у цифровому просторі, що створює нову політичну реальність.

У міжнародних відносинах «культура скасування» також доповнює формальні санкції та спрямована на ізоляцію країни та розрив зв'язків із нею у різних сферах взаємодії, підрив легітимності міжнародного актора. Проблемою реалізації та оцінки прийнятності «культури скасування» в міжнародних відносинах є її невибірковий характер і відсутність єдиної ціннісно-нормативної та інституційної системи, в рамках якої могли б реалізовуватися уявлення про норму та її порушення.

Шляхами нівелювання негативних наслідків від ворожого інформаційного впливу на суспільство та державу в цілому є:

– виважена зовнішня інформаційна політика, мета якої полягає у блокуванні ворожої пропаганди на міжнародній арені;
– в деяких випадках ігнорування інформаційних акцій чи приводів для позбавлення інформаційних джерел «легітимізації» подібних інформаційних акцій;
– впровадження державної системи просвіти населення з питань медіаграмотності;
– створення центрів та започаткування державних проєктів, спрямованих на протидію ворожій дезінформації;
– обмеження кола розповсюдження інформації серед користувачів, тобто вплив на широку громадську думку та електоральні переваги населення за рахунок звуження кола розповсюдження «небажаної» інформації.

Список використаних джерел:

1. В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева, О.Д. Бойко, В.В. Остроухов. Сугестивні технології маніпулятивного впливу: навчальний посібник / за заг. ред. Є.Д. Скулиша.– К.: Наук.– вид. відділ НА СБ України, 2010. 248 с.

2. В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк та ін. Інформаційна безпека (соціально-правові аспекти): підручник / за заг. ред. Є.Д. Скулиша.– К.: КНТ, 2010. 776 с.

3. Simon Kemp. DIGITAL 2024: 5 BILLION SOCIAL MEDIA USERS / DIGITAL 2024: 5 мільярдів користувачів соціальних мереж / We are social / URL: https://wearesocial.com/uk/blog/2024/01/digital-2024–5-billion-social-media-users/ (дата звернення: 25.05.2024)

4. А. Зуйковська. Соціальні мережі, як середовище політичної комунікації. Наукові записки Інституту політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України. 2014. № 1(69). С. 272–280.

5. Т. Савчено-Галушко. Соцмережі стали інструментом маніпулювання інформацією та ведення розвідки ворогом. / АРМІЯ INFORM – онлайн-медіа МОУ.

6. URL: https://armyinform.com.ua/2023/02/28/soczmerezhi-staly-instrumentom-manipulyuvannya-informacziyeyu-ta-vedennya-rozvidky-vorogom/ (дата звернення: 25.05.2024)

7. Social Media Manipulation 2022/2023: Assessing the Ability of Social Media Companies to Combat Platform Manipulation. / NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE. URL: https://stratcomcoe.org/publications/social-media-manipulation-20222023-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/272 (дата звернення: 25.05.2024).

ПИТАННЯ МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ПСИХОЛОГО-ЛІНГВІСТИЧНИХ ЕКСПЕРТИЗ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЩОДО СПРИЧИНЕННЯ ШКОДИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Юлія БРАЇЛКО
кандидат філологічних наук, доцент,
Полтавське відділення ННЦ
«ІСЕ ім. Засл. проф. М.С. Бокаріуса»
Тетяна ЄГОРОВА
Полтавське відділення ННЦ
«ІСЕ ім. Засл. проф. М.С. Бокаріуса»
Наталія КИСЛА
кандидат філологічних наук,
Полтавське відділення ННЦ
«ІСЕ ім. Засл. проф. М.С. Бокаріуса»

Протягом тривалого часу Україна зазнає широкомасштабної збройної та інформаційної агресії з боку Російської Федерації (РФ). Засобами інформаційної агресії поширюють різного роду російську пропагандистську інформацію, яка створює загрозу національній безпеці нашої країни.

Технології російської інформаційно-психологічної спеціальної операції (ІПСО), реалізовані через глобальну мережу «Інтернет» (особливо в соціальних мережах), швидко адаптуються до локальних контекстів українського інформаційного простору, деструктивно впливаючи на внутрішню і зовнішню суспільно-політичну ситуацію в державі. Зменшення критичності сприйняття інформації користувачами інтернету формує підґрунтя для можливих маніпуляцій громадською думкою, сприяє зростанню впливу дезінформації та ворожої пропаганди, популярності конспірологічних теорій, створюючи цим загрози політичній та економічній стабільності України.

Стратегічними цілями російської ІПСО є підрив національної безпеки та національних інтересів України, ліквідація української державності, знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізація суспільно-політичної та соціально-економічної ситуації. На тимчасово окупованих українських територіях, у районах відсічі й стримування збройної агресії РФ розгорнуто безпрецедентну інформаційну кампанію щодо створення альтернативної викривленої інформаційної реальності, побудованої на наративах держави-агресора. Також російська ІПСО постійно маніпулює свідомістю українських громадян, поширюючи, наприклад, міфи та дезінформаційні стереотипи стосовно негативних наслідків вступу України до ЄС і НАТО.

У Законі України «Про національну безпеку України», Стратегії національної безпеки України та Стратегії інформаційної безпеки однією з основних загроз державі визначено інформаційну. З-поміж заходів реалізації Стратегії інформаційної безпеки – залучення науково-дослідних установ, які забезпечують аналітичний та експертний супровід процесу формування і реалізації державної інформаційної політики.

Актуальність науково-практичного вивчення російської ІПСО проти України зумовлена тим, що вона як соціально-психологічна зброя агресора спрямована на досягнення стратегічних цілей – на тектонічні, смислові зсуви в українських культурних, ідеологічних та історичних цінностях.

Російська інформаційна війна проти України є центром уваги вітчизняних політиків і вчених (з-поміж них – Є. Магда, Г. Почепцов, М. Дзюба та ін.), які зазначають, що смисли, інтегровані у свідомість українських людей, програмують моделі поведінки для виконання довгострокових стратегічних завдань РФ.

Думку політиків і вчених потвердила дійсність: протягом десятиріч, особливо від початку повномасштабного вторгнення РФ в Україну, українське населення піддано масованим атакам російської ІПСО, метою якої є підтримка російської збройної агресії, схвалення тимчасової окупації окремих територій України, спонукання до співпраці з державою-агресором і з окупаційною владою тощо. Арсенал ІПСО охоплює штучні, пропагандистські політичні терміни, імплантуючи в індивідуальну свідомість українських людей російську ідеологічну матрицю, поширювану інтернет-ресурсами, телекомунікаціями та навіть закладами освіти (наприклад, «проект Новороссия», «бандеровщина», «украинские нацисты», «фашизм на Украине», «Россия – освободитель украинского народа» та ін.).

У чинному законодавстві України поняття «інформаційна безпека» охоплює багато складників, з-поміж яких – лінгвістичні та психологічні чинники, які мають суттєве доказове значення для правової кваліфікації кримінальних правопорушень, що завдають шкоди інформаційній безпеці держави [1–4].

Експерти Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» (далі – ННЦ ІСЕ) та його територіальних відділень зокрема виконують велику кількість комплексних судових психолого-лінгвістичних експертиз, призначених у кримінальних провадженнях, уключених до Розділу І Особливої частини Кримінального кодексу України («Злочини проти основ національної безпеки України»): ст. 109 («Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади»), ст. 110 («Посягання на територіальну цілісність і недоторканність України»), ст. 111 («Державна зрада»), ст. 1111 («Колабораційна діяльність»), ст. 1142 («Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану»).

Як свідчить експертна практика, проведення комплексної психолого-лінгвістичної експертизи за кримінальними правопорушеннями щодо заподіяння шкоди інформаційній безпеці України сьогодні зазнає труднощів через відсутність методичних розробок. Це значно ускладнює виконання таких комплексних досліджень, нерідко призводячи до розпливчатості та еклектичності експертних завдань, до виходу за межі компетенції експертів, до алогічності та до неаргументованості експертних висновків тощо. Порушення доказовості, об'єктивності, повноти дослідження, вихід за межі компетенції суперечать основоположним принципам і регламенту судово-експертної діяльності, передбаченим чинним законодавством України [5–7].

Сьогодні назріла нагальна необхідність розроблення теоретичних та методичних засад комплексної психолого-лінгвістичної експертизи з метою виконання надважливих завдань, що стосуються реалізації державної інформаційної політики та інформаційної безпеки України.

Фахівці ННЦ ІСЕ вперше розробили методичні рекомендації з комплексного психолого-лінгвістичного дослідження у кримінальних провадженнях щодо спричинення шкоди інформаційній безпеці держави (далі – Методичні рекомендації).

Теоретичною та методологійною базою розроблення Методичних рекомендацій стали роботи науковців у галузях судової експертології, лінгвістики, психології; емпіричною базою – матеріали кримінальних проваджень щодо завдання шкоди інформаційній безпеці держави; статистичні дані, отримані з відкритих джерел інформації; практика проведення комплексних психолого-лінгвістичних експертиз, призначених у відповідних кримінальних провадженнях.

Методичні рекомендації розроблено з опертям на синкретизм методології лінгвістичного й психологічного досліджень. Комплексне психолого-лінгвістичне дослідження є відносно новим у вітчизняній практиці судової експертизи. На перших етапах його становлення об'єкт психолого-лінгвістичного дослідження традиційно визначали як текст, що є продуктом мов-

леннєвої комунікативної діяльності, об'єднаний сенсом, структурною цілісністю, змістовою зв'язністю і завершеністю (наприклад, книги, статті, договори, заяви, записки, нотатки тощо). З розвитком віртуального соціального середовища й технологічних можливостей інтернету діапазон об'єктів комплексного психолого-лінгвістичного дослідження значно збільшився, тому експертне вивчення тільки тексту стало недостатнім для розв'язання актуальних завдань досудового розслідування та суду.

Зокрема, із масовим розповсюдженням цифрових носіїв інформації, здатних фіксувати відеозапис, збільшилася потреба в психологічному аналізі комбінованого (мультимодального) інформаційного об'єкта в аспекті взаємозв'язків та ієрархії вербального й невербального компонентів комунікації. Новітніми для психолого-лінгвістичного дослідження стали медійні тексти з ілюстративними зображеннями, медіатексти (наприклад, статті в інтернет-ЗМІ), а також варіації віртуальної комунікації в соціальних мережах і месенджерах (аудіо- та відеоролики без коментарів, текстові й голосові повідомлення, скриншоти, коментарі користувачів інтернету тощо).

Отже, нові об'єкти, що містять інформаційний матеріал, в аспекті їхньої комунікативної функції вийшли за межі традиційного текстового формату й набули характеристик, що потребують для свого вивчення об'єднання знань у галузях лінгвістики та психології. У Методичних рекомендаціях окреслено основні принципи, об'єкт, предмет, завдання, методи та алгоритми комплексного психолого-лінгвістичного дослідження в кримінальних провадженнях щодо спричинення шкоди інформаційній безпеці держави.

Ці рекомендації будуть корисними для науковців і судових експертів, які проводять дослідження на базі інтеграції спеціальних лінгвістичних і психологічних знань, що мають доказове значення в процесі розслідування кримінальних правопорушень щодо завдання шкоди інформаційній безпеці держави.

Список використаних джерел:

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2469–19#Text (дата звернення: 12.06.2024).

2. Стратегія національної безпеки України. Безпека людини – безпека країни: рішення Ради національної безпеки і оборони України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/card/392/2020 (дата звернення: 12.06.2024).

3. Стратегія інформаційної безпеки: рішення Ради національної безпеки і оборони України від 15.10.2021 р. URL: https://www.president.gov.ua/documents/6852021–41069 (дата звернення: 12.06.2024).

4. Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/card/2341–14 (дата звернення: 12.06.2024).

5. Про судову експертизу: Закон України від 540 25.02.1994 р. № 4038-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4038–12#Text (дата звернення: 12.06.2024).

6. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: http://zakon.rada.gov.ua/laws/show/4651–17 (дата звернення: 12.06.2024).

7. Інструкція про призначення та проведення судових експертиз та експертних досліджень: затв. наказом Мін'юсту України від 08.10.1998 h/ № 53/5) (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705–98#Text (дата звернення: 12.06.2024).

КІБЕРОПЕРАЦІЯ У СУЧАСНІЙ ВІЙНІ: МЕЖІ ЗАСТОСУВАННЯ ЧЕРЕЗ ПРИЗМУ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА

Ілля ВДОВІН
співробітник СБУ

Майже два з половиною роки протистояння українського суспільства безпрецедентній за своїми формами, масштабами та методами глобальній агресії зі сторони російської федерації, змусило світову спільноту ініціювати перегляд існуючих власних військових доктрин, адаптувати нормативи щодо застосування збройних сил відповідно до актуальних реалій сучасних театрів бойових дій, як в обороні, так і в активному наступі.

Одним із основних компонентів формування сучасних тенденцій військового мистецтва є науково-технічний прогрес, який в свою чергу, кардинально змінює характер планування та виконання традиційних військових операцій. Саме завдяки науково-технічному прогресу поле ведення бойових дій, окрім звичайних наземного, повітряного та морського, перемістилося також до кібернетичого простору. При цьому, застосування та наслідки проведених кібероперацій в деяких випадках можуть нести більш руйнівну силу, ніж застосування «класичного» озброєння, що базується на кінетичному принципі дії.

Практика російсько-української війни слугує доказом того, що комплекс застосованих кібератак за характером своєї руйнівної сили та впливом на відповідні об'єкти або навіть цілі галузі критичної інфраструктури, може призвести до значно масштабніших наслідків ніж надсучасна та високо-технологічна зброя. Окрім матеріалізованих наслідків впливу на ціль, кібернетичний напад може бути спрямованим на завдання масованого психологічного впливу на цілі групи населення та суспільство в цілому, порушення штатного режиму використання встановлених систем комунікації, розриву механізмів забезпечення життєдіяльності населення країни, спричинення іншого негативного впливу.

Характерною рисою, що відрізняє природу застосування кібернетичної зброї від кінетичної – це фактична можливість використання методів проведення кібероперацій до початку «відкритих» бойових дій, що, в свою чергу, безпосередньо спостерігалось в українському кіберпросторі напередодні 24 лютого 2022 року.

Ускладнена через комплексні технічні особливості атрибуція кібератаки сприяє розробці, плануванню та застосуванню вказаних руйнівних заходів вже у мирний час, тобто без фактичного оголошення стану війни, відповідно до вимог та площини правового регулювання міжнародним гуманітарним правом (МГП).

Зловживання можливостями кіберпростору та застосування проти «країни-цілі» (ряду країн, політично-військового об'єднання, тощо) кібероперації надає відчутні переваги в економічній, дипломатичній та військовій сферах навіть без формального порушення кордонів та суверенітету. В деяких випадках, вдало спланована та застосована масштабна кібероперація може вплинути також на демократичні інститути країни: порушити об'єктивність проведення виборчого процесу або забезпечити вплив на результати плебісциту.

Таким чином зброя, що застосовується у кіберпросторі має очевидні переваги, які зумовлені найбільшою здатністю самовдосконалення атакуючих засобів, географічною незалежністю наступальних дій, специфікою атрибуції атакуючої сторони, та необмежено ефективними можливостями застосування.

Не дивлячись на те, що за своїми руйнівними можливостями, кібератака може навіть переважати кінетичні засоби ураження, міжнародне гуманітарне право лише поверхнево торкається меж застосування та використання вказаного сучасного виду озброєння та залишається практично зосередженим лише на спробі унормування «класичних» звичаїв та правил ведення війни.

Звісно, специфіка та особливості кібервійни не дозволяє зробити пряму проєкцію застосування норм МГП щодо її суб'єктів та вчинюваних останніми об'єктивних дій. Зокрема, на основі аналізу міжнародних документів – Женевських конвенцій та Додаткових протоколів до них [1], виокремлено основні ознаки комбатантів та цивільного населення відповідно до міжнародного права, визначено обсяг їхніх прав та обов'язків, а також підстави для притягнення до кримінальної відповідальності. Так, основною ознакою комбатанта є його перебування у збройних силах. Пункт 2 ст. 43 Протоколу І визначає, що збройні сили сторони, яка перебуває в конфлікті, складаються з усіх організованих збройних сил, груп і підрозділів, що перебувають під командуванням особи, відповідальної перед цією стороною за поведінку своїх підлеглих, навіть якщо ця сторона представлена урядом чи владою, невизнаними супротивною стороною. Такі збройні сили підпорядковані внутрішній дисциплінарній системі, яка забезпечує додержання норм міжнародного права, застосовуваних у період збройних конфліктів [2].

Отже ми бачимо, що навіть на рівні лише поверхневого аналізу зазначених норм МГП стає зрозумілою фактична неможливість ідентифікації та визначення учасників кібератаки за стандартними критеріями віднесення до статусу комбатантів або ж до цивільного населення.

Зокрема, учасниками кібероперації та особами, що залучені до вчинення кібератаки можуть виступати суб'єкти, які взагалі не мають відношення до військових формувань чи мілітарізованих утворень, перебувають за межами країни в якій здійснюються розробка та управління кібероперацією, або ж взагалі – абсолютно анонімізовані, як по відношенню до центру планування кібератаки, так і у зворотньому напрямку.

Кіберактивність піддається анонімності за допомогою кількох рівнів абстракції. Наприклад, кібероперація може бути розпочата громадянином держави А з території держави Б і націлена на державу С. Громадянин держави А може використовувати різні методи в місці виникнення, щоб приховати свою особистість, а також спрямувати операцію через будь-яку кількість країн та інфраструктур між початком операції в державі Б та її ціллю – державою С.

Так само спірним є питання щодо кваліфікації дій, пов'язаних із порушенням суверенітету «країни-цілі» внаслідок застосованої щодо неї кібероперації. Зауважимо, що кіберпростір – складне, багаторівневе середовище, до якого юридичні ознаки поняття «суверенітету» не можуть бути застосовані в класичному розумінні зазначеної категорії.

За своєю суттю кіберпростір не обмежується штучно сконструйованим комп'ютеризованим середовищем, адже постійно розвивається та є глобалізованим, постійно змінюється й може бути використаний будь-ким для будь-яких цілей. Кібернетичний суверенітет також відрізняється тим, що базові фізичні елементи повністю створені людиною, а ризиками і вразливими місцями в кіберпросторі можна керувати або пом'якшувати шляхом маніпулювання самим доменом.

Водночас, наскільки б кіберпростір не був інтегрований у середовище, що не має чітких географічних та фізичних меж – результати здійснених у ньому кібератак завжди досягають конкретних матеріалізованих наслідків. Останні, в свою чергу можуть чітко виражатися або у майновій оцінці, або навіть призводити до летальних випадків як серед комбатантів, так і серед цивільного населення.

Кібероперація, що спланована проти об'єкта військової інфраструктури, або ж направлена на спричинення прямих втрат серед особового складу воєнізованих формувань супротивника, може також нанести шкоду об'єктам цивільного життєзабезпечення, або призвести до тяжких наслідків серед мирного населення. Так, спричинена за результатами кібератаки, зупинка штатної роботи електрогенеруючої станції може припинити живлення не тільки військової частини, але й закладів охорони здоров'я, освіти, тощо, а завдання, наприклад, шкоди системам комунікації, окрім порушення режиму зв'язку між військовими формуваннями, буде синхронно завдавати шкоди мирному використанню цих засобів.

З урахуванням викладеного, порядок застосування положень міжнародного гуманітарного права під час планування кібероперацій, як і визначення статусу «законної цілі», що підлягає кібератаці є дещо розмитими та, у певній мірі, нормативно неврегульованими. За таких умов,

фактично нівелюється можливість надання фахівцями-юристами вищевказаної галузі права вірної консультації оперативним штабам планування з приводу допустимості проведення кібероперацій стосовно того чи іншого об'єкту ураження.

Значним кроком до розв'язання вказаної проблематики була ініціатива Об'єднаного центру передових технологій з кібероборони НАТО (м. Таллінн, Естонська Республіка), який у 2009 році зібрав міжнародну групу вчених-юристів і практиків для розробки посібника, в якому розглядається тлумачення міжнародного права в контексті кібероперацій і кібервійни.

Результатом діяльності правників стало «Талліннське керівництво із застосування міжнародного права до кібероперацій» (періодично доповнюється та редагується) [3], що фактично хоч і не являється нормативним документом, або правовою підставою, згідно якої уряди можуть вживати будь-яких заходів у відповідь на законну або незаконну кібердіяльність, однак містить набір рекомендацій та правових думок спеціалістів країн євроатлантичної спільноти з вказаного приводу.

Наразі «Талліннське керівництво із застосування міжнародного права до кібероперацій» охоплює повний спектр міжнародного права, що застосовується до кібероперацій, починаючи від правових режимів у мирний час і закінчуючи правом збройних конфліктів, а також широким спектром принципів міжнародного права і режимів, які регулюють події в кіберпросторі. Деякі з них стосуються загального міжнародного права, наприклад, принципу суверенітету та різних підстав для здійснення юрисдикції.

Також у вищевказаному документі детально розглядається питання державної відповідальності, що включає в себе правові норми атрибуції. Крім того, наводяться численні спеціалізовані режими міжнародного права, включаючи право прав людини, повітряне та космічне право, морське право, а також дипломатичне та консульське право в контексті кібероперацій. Окрім вказаного, керівництво визначає розширений спектр норм, що регулюють кібероперації, і надає розгорнуті коментарі до них.

Таким чином, можемо підсумувати, що наукова думка та науковий погляд фахівців-правників крокує значно попереду, а ніж спроби дійсного юридичного врегулювання питання меж використання кіберопрацій у площині міжнародного гуманітарного права. Сподіваємось, що українські правники у вказаній сфері, маючи, нажаль, практичний досвід з огляду на повномасштабну агресію російської федерації, внесуть свій вклад у формування спільної правової позиції країн цивілізованого світу, а також закладуть основу для створення майбутньої міжнародно-правової бази з означених питань.

Список використаних джерел:

1. Додатковий протокол до Женевських конвенцій від 12.08.1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол I) від 08.06.1977 р. Верховна Рада України. Законодавство України. URL: https://goo.gl/WjGDUL (дата звернення 17.06.2024).

2. Конвенція про захист цивільного населення під час війни від 12.08.1949 р. Верховна Рада України. Законодавство України. URL: https://goo.gl/RWysku (дата звернення 17.06.2024).

3. Шмітт, Майкл Н. Талліннський посібник з міжнародного права, що застосовується до кібервійни. Нью-Йорк, Сполучені Штати Америки: Видавництво Кембриджського університету, 2013.

ОБ'ЄКТИВНІ ПЕРЕДУМОВИ МІЖНАРОДНОЇ СПІВПРАЦІ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Олексій ГІЧКО
аспірант Державної наукової установи
«Інститут інформації, безпеки і права
Національної академії правових наук України»

Актуальність питань міжнародного співробітництва держав в інформаційній сфері обумовлена, перш за все, збільшенням залежності всіх галузей життя сучасного суспільства від розвитку та функціонування інформаційних технологій. Впровадження новітніх інформаційних можливостей і засобів спілкування, що об'єднують суб'єктів міжнародної комунікації, з одного боку, відкриває колосальні перспективи розвитку суспільства, з іншого ж, виявляє численні проблеми політичного, соціально-економічного, науково-технічного, військового і правового характеру. Вирішення означених проблем в більшості випадків полягає в площині спільних зусиль суб'єктів міжнародного співтовариства та їх представників, з урахуванням взаємовигідного співробітництва між державами.

В науці термін «міжнародне співробітництво» визначається в цілому як універсальна форма організації спільного або взаємоузгодженого виробництва за участю іноземних партнерів двох або декількох країн, заснована на розподілі виробництва продукції, комерційному співробітництві, взаємній гарантії ризиків, спільному захисті інвестицій і промислових секретів [1, с. 45].

Окремі дослідники головними напрямами сучасної міжнародної інформаційної політики визначали сприяння міжнародному співробітництву в комунікаційній сфері, заохочення до міжнародного обміну інформацією незалежно від кордонів і рівноправну участь у міжнародних інформаційних потоках, використання глобальної економічної інтеграції на основі міжнародної інфоінфраструктури в національних інтересах, об'єднання інтелектуальних ресурсів різних країн для прогресивного розвитку цивілізації [2, с. 102]. І дійсно, участь тієї або іншої держави в світових інформаційних потоках, по-перше, є запорукою зміцнення її технологічного потенціалу та здатністю збагачувати свою інформаційну сферу надбаннями як наукового, так і політичного, економічного, культурного характеру, а, по-друге, можливістю оперативно реагувати на глобальні зміни в світі. Від цього залежить авторитет держави на світовій арені, а також можливість повною мірою забезпечити захист і охорону інформаційної безпеки як складової національної безпеки в цілому.

По великому рахунку, відносини, які виникають в інформаційній сфері, як правило, супроводжують інші процеси, які є важливими для розвитку суспільства та реалізації ним своїх найважливіших свобод та інтересів. А тому, як зазначає К.А. Дубняк, інформаційна сфера, разом з її інформаційними полями та потоками, завдяки своїй динамічності й гнучкості є рушієм розвитку постіндустріального суспільства та активно впливає на стан економічної, політичної, оборонної й інших складових національної безпеки. Більше того, кіберпростір стає одним з основних об'єктів уваги держав, які тримають «руку на пульсі» розвитку національних інформаційних просторів і при цьому надають їх суб'єктам можливість для розвитку, що потребує подальших досліджень [3, с. 24]. Таким чином, однією із передумов міжнародної співпраці нашої держави в інформаційній сфері є необхідність розвитку суспільства та реалізації ним окремих прав, свобод та інтересів, які стосуються інформаційної сфери.

Така якість нашої країни, як здатність виступати рівноправним учасником певних відносин на міждержавному рівні, напряму пов'язана із її суверенітетом, як невід'ємною ознакою будь-якої держави. Скрипнюк О.В. та Крусян А.Р., наприклад, визначають державний суверенітет як політико-юридичну властивість сучасної держави, що виражається у верховенстві її влади всередині країни та незалежності зовні. Він безпосередньо пов'язаний з суверенною державною владою, характеризується самостійністю щодо вирішення питань у політико-пра-

вовій сфері та верховенством державної влади у відносинах з іншими видами соціальної влади; характеризується неподільністю та єдністю і не може бути поділеним між іншими суб'єктами політико-правових відносин; означає незалежність і рівноправність держави у зовнішніх відносинах. Суверенною є та держава, яка володіє зовнішнім і внутрішнім суверенітетом [4, с. 16–17]. Олєйніков Д.О. вважає, що суверенітет держави в інформаційній сфері (інформаційний суверенітет) характеризує верховенство, самостійність, повноту і неподільність влади України в межах її інформаційного простору та незалежність і рівноправність у зовнішніх зносинах, пов'язаних із реалізацією інтересів в інформаційній сфері. При цьому інформаційний суверенітет є складовою державного суверенітету та, у свою чергу, містить 2 складові – внутрішню та зовнішню [5, с. 66–67]. Також під інформаційним суверенітетом України розуміється її виключне право відповідно до Конституції і законодавства України та норм міжнародного права самостійно і незалежно з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні й геополітичні національні інтереси в інформаційній сфері, державну внутрішню й зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави [6].

За визнанням створеної в рамках ООН Групи урядових експертів щодо досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки, «суверенітет держав і міжнародні норми та принципи, що слідують із суверенітету, застосовуються до здійснення державами діяльності, пов'язаної з ІКТ [інформаційно-комунікаційними технологіями], та до їх юрисдикції над ІКТ-інфраструктурою, розташованою на їх територіях. У процесі використання ІКТ держави повинні дотримуватися, поряд з іншими принципами міжнародного права, таких принципів, як державний суверенітет, суверенна рівність, вирішення спорів мирними засобами та невтручання у внутрішні справи інших держав» [7]. Таким чином, на рівні міжнародної спільноти офіційно визнано поширення суверенітету держави на питання, пов'язані з інформаційною сферою, що дає потенційну можливість відповідним суб'єктам мати певні права і свободи в інформаційній сфері, а також реалізовувати їх. Вважаємо суверенітет держави в інформаційній сфері також однією з передумов міжнародної співпраці у цій сфері.

В сучасних умовах поглиблення співпраці України з НАТО задля набуття членства в цій організації координація діяльності органів виконавчої влади, ЗМІ тощо з питань співробітництва з НАТО в інформаційній сфері відіграє все більшого значення. Цей вектор розвитку зовнішньої політики України впливає й на правове регулювання системи безпеки інформації як складової частини євроатлантичного безпекового простору [8, с. 110]. На думку В.С. Політанського, країни Європи, що входять до НАТО, є найбільш успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства [9, с. 35]. Означені обставини обумовлюють необхідність досить предметного розуміння сутності інформаційної політики та змісту інформаційного простору вказаних країн, а також виділення перспективних напрямків, в яких можлива плідна співпраця з ними.

Окремі дослідники головними напрямами сучасної міжнародної інформаційної політики визначали сприяння міжнародному співробітництву в комунікаційній сфері, заохочення до міжнародного обміну інформацією незалежно від кордонів і рівноправну участь у міжнародних інформаційних потоках, використання глобальної економічної інтеграції на основі міжнародної інфоінфраструктури в національних інтересах, об'єднання інтелектуальних ресурсів різних країн для прогресивного розвитку цивілізації [10, с. 102]. І дійсно, участь тієї або іншої держави в світових інформаційних потоках, по-перше, є запорукою зміцнення її технологічного потенціалу та здатністю збагачувати свою інформаційну сферу надбаннями як наукового, так і політичного, економічного, культурного характеру, а, по-друге, можливістю оперативно реагувати на глобальні зміни в світі. Від цього залежить авторитет держави на світовій арені, а також можливість повною мірою забезпечити захист і охорону інформаційної безпеки як складової національної безпеки в цілому.

По великому рахунку, відносини, які виникають в інформаційній сфері, як правило, супроводжують інші процеси, які є важливими для розвитку суспільства та реалізації ним своїх найважливіших свобод та інтересів. А тому, як зазначає К.А. Дубняк, інформаційна сфера, разом з її інформаційними полями та потоками, завдяки своїй динамічності й гнучкості є рушієм розвитку постіндустріального суспільства та активно впливає на стан економічної, політичної, оборонної й інших складових національної безпеки. Більше того, кіберпростір стає одним з основних об'єктів уваги держав, які тримають «руку на пульсі» розвитку національних інформаційних просторів і при цьому надають їх суб'єктам можливість для розвитку, що потребує подальших досліджень [3, с. 24]. Таким чином, однією із передумов міжнародної співпраці нашої держави в інформаційній сфері є необхідність розвитку суспільства та реалізації ним окремих прав, свобод та інтересів, які стосуються інформаційної сфери.

Таким чином, України фактично має сформований інформаційний простір, а також розвинену структуру інформаційної сфери, яку використовує в межах реалізації власних інтересів як в межах держави, так і в межах зовнішніх відносин. І найважливішою передумовою міжнародної співпраці України з іншими суб'єктами є потреба в реалізації національних інтересів в інформаційній сфері. Доктриною Інформаційної безпеки, затвердженою Указом Президента України від 25 лютого 2017 року № 47/2017 [11], визначено перелік національних інтересів України в інформаційній сфері. До них віднесені наступні:

1. Життєво важливі інтереси особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів.

2. Життєво важливі інтереси суспільства і держави: захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації; захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України; всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації; забезпечення вільного обігу інформації, крім випадків, передбачених законом; розвиток та захист національної інформаційної інфраструктури; збереження і примноження духовних, культурних і моральних цінностей Українського народу; забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України; вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування; зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності; розвиток медіа-культури суспільства та соціально відповідального медіа-середовища; формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів; створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди; розвиток інформаційного суспільства, зокрема його технологічної інфраструктури; безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір; розвиток системи стратегічних комунікацій України; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері; забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України; захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом; формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти; розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

Сучасна міжнародна співпраця в інформаційній сфері здійснюється на договірній основі, а за відсутності договорів – на засадах взаємності, у межах міжнародних організацій, через представників державних органів, у регіональному масштабі. Вказана діяльність ґрунтується на системі правового регулювання взаємодії держав, їх компетентних органів та інших суб'єктів, яка заснована на взаємодії міжнародного та національного права, що регулюють відносини в інформаційній сфері.

Список використаних джерел:

1. Кирєєва А.Є. Міжнародне співробітництво в сфері інформаційно-комунікаційних технологій. Глобальні та національні проблеми економіки. 2015. Випуск 8. С. 44–51.

2. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.]; НАН України, Нац. б-ка України ім. В.І. Вернадського. К.: НБУВ, 2011. 154 с.

3. Дубняк К.А. Інформаційний простір: структура та функціональні параметри. Держава та регіони. Серія: Соціальні комунікації, 2015 р., № 4 (24). С. 21–25.

4. Скрипнюк О.В., Крусян А.Р. Концепт «державний суверенітет» у класичних західних теоріях. Альманах права. 2021. Вип. 12. С. 11–19.

5. Олєйніков Д.О. Зміст та складові інформаційного суверенітету як об'єкта кримінально-правової охорони. Геополітичні пріоритети України. Збірник наукових праць. 2021. Вип. 1 (26). С. 60–69.

6. Концепція інформаційної безпеки (проєкт) [Електронний ресурс] – Режим доступу: https://www.osce.org/files/f/documents/0/2/175056.pdf. (дата звернення: 15.06.2024)

7. Доповідь Групи урядових експертів по досягненням у сфері інформатизації і телекомунікацій в когнтексті міжнародної безпеки 2015 г.– С. 16.– Mode of access: http://undocs.org/ru/A/70/174. (дата звернення: 15.06.2024)

8. Костенко О.В. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури/ О. Костенко. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 34, том 3. 2015. С. 109–114.

АЛГОРИТМІЗАЦІЯ ДОСЛІДЖЕННЯ ВИРОКІВ ЗА СТ. 438 КК УКРАЇНИ

Ірина ГЛОВЮК
докторка юридичних наук, професорка,
професорка кафедри
кримінально-правових дисциплін
Інституту права Львівського державного
університету внутрішніх справ

Зважаючи на те, що елементом перехідного правосуддя є і розслідування та судовий розгляд порушень законів та звичаїв війни, то важливо постійно здійснювати аналіз судових рішень за ст. 438 КК України через специфіку цього злочину та тригерність фактів вчинення воєнних злочинів.

З урахуванням рекомендацій міжнародних та національних експертів [1, с. 81, 771–775] вже було сформульовано важливі специфічні аспекти викладу для вироків за ст. 438 КК України:

– по-перше, відображати вичерпний перелік порушень норм міжнародного гуманітарного права із посиланням на те, які саме норми порушено (у ст. 438 КК України іде мова про міжнародні договори), і особливо – для форми «інші порушення законів та звичаїв

війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України»;
- по-друге, вказувати на захищений статус жертви / об'єкта за міжнародним гуманітарним правом (якщо це має місце);
- по-третє, прописувати усвідомлення виконавцем існування збройного конфлікту та зв'язку діяння зі збройним конфліктом (у тому числі і усвідомлення захищеного статусу жертви / об'єкта за міжнародним гуманітарним правом). Відсутність такого зв'язку виключає кваліфікацію за ст. 438 КК України.

І ці позиції мають бути відображені таким чином, щоб, по-перше, було зрозуміло, яке саме порушення норм міжнародного гуманітарного права вчинив обвинувачений (засуджений), по-друге, вжиті формулювання виключали будь-яке протилежне розуміння фактичних обставин та їх юридичної оцінки [2].

Утім, важливою є розробка алгоритму аналізу (дослідження) вироків за ст. 438 КК України, який може бути корисним для цілей оскарження та перевірки судових рішень, так і для доктринальної експертної оцінки.

Пропонований авторський алгоритм складається з двох частин: 1) загальний аналіз (дослідження) вироку (є спільним для вироку за будь-якою статтею КК України); 2) аналіз у аспекті специфіки ст. 438 КК України. Зважаючи на те, що загальний аналіз не має особливостей за ст. 438 КК України, увага буде зосереджена на другій частині.

Алгоритм аналізу може мати таку послідовність:

1) Виклад контекстуального елементу у описі фактичних обставин. Зокрема, йдеться про опис ситуації збройного конфлікту та участі обвинуваченого (засудженого, виправданого) у цьому збройному конфлікті, зв'язку дій обвинуваченого (засудженого, виправданого) та збройного конфлікту. Слід відмітити, що у судовій практиці є кардинально різні підходи до обсягу опису контекстуального елементу саме у цьому аспекті [3–6], який, до того ж, змінюється з розвитком судової практики щодо злочину порушення законів та звичаїв війни [7]. Що ж стосується усвідомлення фактичних обставин, які свідчать про існування збройного конфлікту, то воно може бути викладено як при описі фактичних обставин, так і у інших частинах вироку. Наприклад: у суду немає сумнівів в розумінні обвинуваченим ОСОБА_3, як кадровим військовим рф, законів і звичаїв війти, що передбачені міжнародними договорами, факту незаконного перетину державного кордону України, участі у військовій агресії проти України, враховуючи показання потерпілого ОСОБА_6 та свідків ОСОБА_8, ОСОБА_7, про те, що обвинувачений ОСОБА_3 перебував у військовій формі, зі зброєю, надавав накази та спілкувався з приводу своїх подальших дій з іншими особами, які перебували на місці події також у військовій формі, зі зброєю. При цьому, стороною обвинувачення надані письмові докази перебування обвинуваченого у складі збройних сил російської федерації [8].

2) Опис порушених норм міжнародного гуманітарного права. Незважаючи на формальну легкість, проведений аналіз вироків демонструє, що є певні питання. Зокрема, вони торкаються: уточнення конкретних порушених норм МГП (а не просто переліку статей ЖК або ДП І); уточнення форми порушення, якщо у статті або частині статті їх кілька; опис захищеного статус осіб або об'єктів. Крім того, має бути перевірено, чи зазначені джерела міжнародного права, що визнають порушення міжнародного гуманітарного права воєнними злочинами (наприклад, конкретні положення чотирьох Женевських конвенцій або Додаткового протоколу І, які стосуються серйозних порушень, стаття 8 Статуту МКС та/ або статті 2 і 3 Статуту МКТЮ, які кодифікують міжнародне звичаєве право тощо) [1, с. 771]. Зважаючи на доктринальну складність питання про ст. 438 КК України та серйозність порушень норм міжнародного гуманітарного права, навряд буде правильно кваліфікувати як помилку окремого обґрунтування серйозності порушень, якщо це порушення є у переліку ЖК та ДП І і про це прямо зазначено у вироку. Утім, відмітимо, по-перше, що такі аналізи є у деяких вироках (зокрема, по ситуації погрози вбивством та нанесення удару прикладом автомату цивільному населення та привласнення мобільного телефону [8]; або по ситуації заволодіння приватним майном цивільного

населення [9]), по-друге, він є необхідним у деяких випадках. Про це пише М.І. Пашковський: серйозність порушення МГП, якщо воно не міститься в одному з переліків ст.ст. 50 ЖК(I), 51 ЖК(II), 130 ЖК(III), 147 ЖК(IV), 85 Протоколу I, повинна окремо обґрунтовуватися в процесуальних рішеннях через порушення норми, яка захищає важливі цінності, і тяжкість наслідків такого порушення для жертви [10, с. 124].

3) Формулювання обвинувачення, визнаного судом доведеним. По-перше, слід звернути увагу на чіткість викладення об'єктивної сторони. Це особливо важливо, коли йдеться про «інші порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України»: має бути прописано, у чому полягає це порушення, щоб було очевидно, що воно не підпадає під інші форми об'єктивної сторони. По-друге, якщо мова йде про такі порушення, які являють собою декілька форм об'єктивної сторони, вони мають бути чітко розмежовані у контексті диспозиції ст. 438 КК України; це, як правило, характерне для жорстокого поводження з цивільним населенням та інших порушень законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України. По-друге, слід звертати увагу на характер опису порушень норм саме МГП. Дещо невиправдано лаконічними видаються формулювання на кшталт «Порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України». Більш правильними видаються формулювання, де міститься посилання не лише на ст. 438 КК України, а й на конкретний зміст положень МГП, хоча б у контексті конкретних порушених норм МГП. Зокрема, гарним прикладом є формулювання: порушення законів та звичаїв війни, передбачених міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, що виразилось у порушенні вимог ст. 147 Женевської Конвенції про захист цивільного населення під час війни від 12.08.1949, яка набрала чинності для України 03.01.1955, які полягають у примушуванні осіб, що перебувають під захистом, служити в збройних силах держави окупанта [11]. Дискусійним питанням є можливість посилання на РС МКС, і вже зроблено висновок, що посилання на Римський Статут МКС не може бути елементом формулювання обвинувачення або правової кваліфікації діяння [12, с. 99].

4) Правова кваліфікація діяння. З одного боку, мова йде лише про статтю 438 КК України. З іншого боку, вона є бланкетною, і обсяг і зміст статті 438 КК України не є чітко визначеними. Як наслідок, слід мати на увазі, що злочини, перелічені у статті 438, не завжди є ідентичними діянням, що лежать в основі воєнних злочинів, кодифікованих за міжнародним кримінальним правом. У деяких випадках правопорушення, передбачені статтею 438, можуть охоплювати одне або кілька діянь, що лежать в основі воєнних злочинів, а в інших випадках діяння, що лежать в основі воєнних злочинів, можуть одночасно належати до різних компонентів статті 438 [1, с. 81]. У цьому ж аспекті є слушні зауваження щодо «невтрати» посилань на ст. 28 КК України у випадку співучасті, а випадки вчинення воєнних злочинів у співучасті, на жаль, поширені. Адже, як зазначають дослідниці, у деяких вироках, де фігурує виключно військовий начальник зс рф, який за доведеним обвинуваченням віддавав накази своїм підлеглим, військовослужбовцям зс рф, порушити закони та звичаї війни, його дії так само зі ставленням у вину того порушення законів або звичаїв війни, що було вчинено підлеглими та які становили зміст наказу чи розпорядження, кваліфікувалися лише за ч. 1 ст. 438 КК, без посилання на ч. 2 ст. 438 КК. А вчинення злочину у співучасті (за попередньою змовою групою осіб) не враховувалося судом при призначенні покарання такому військовому начальнику [13, с. 116]. Очевидно, що таких помилок не має бути. Крім того, слід розмежовувати відповідальність командирів та командну відповідальність [детальніше див.: 14–16] при кваліфікації.

5) Докази на підтвердження встановлених судом обставин. При аналізі цього блоку вироків слід керуватися такими рекомендаціями експертів: а) мають бути зазначені правові елементи складу воєнних злочинів, а також правовий аналіз того, як кожен з цих елементів було встановлено у конкретній справі [1, с. 773]; б) судді повинні відзначити кожну з контекстуальних вимог у вироку та пояснити, чи доведена кожна з них у конкретній справі, і якщо так,

то в який спосіб [1, с. 775]. Як видно, є вимога окремого пояснення способу (шляху) доведення у провадженні, що не цілком звичним для нашої правової системи, зважаючи на те, що йдеться про правові елементи складу воєнних злочинів: контекстуальний елемент, actus reus, mens rea. Найбільш доречним, хоча і незвичним для вироків по ординарним злочинам, є окрема характеристика у мотивувальні частині саме цих елементів, навіть без згадування їх іншомовних назв. Цікавий приклад такого викладу вже є, при цьому у вироку написано буквально наступне: «Отже, судом встановлені наступні обставини» [17].

6) Дотримання гарантій захисту. Якщо вирок постановлено у режимі спеціального судового провадження, то має бути проаналізовано, чи дотримано умови застосування спеціального судового провадження; як відображено у вироку повідомлення про судовий розгляд; як забезпечено участь захисника та чи є ознаки неефективного захисту. Тобто як дотримано ч. 5 ст. 374 КПК України: у разі ухвалення вироку за наслідками кримінального провадження, у якому здійснювалося спеціальне досудове розслідування або спеціальне судове провадження (in absentia), суд окремо обґрунтовує, чи були здійснені стороною обвинувачення всі можливі передбачені законом заходи щодо дотримання прав підозрюваного чи обвинуваченого на захист та доступ до правосуддя з урахуванням встановлених законом особливостей такого провадження. У проаналізованих вироках цьому приділяється увага, хоча ці обставини розписуються з різним обсягом деталізації.

Висновок. Запропоновано алгоритм дослідження вироків за ст. 438 КК України з такою послідовністю аналізу:

- викладу контекстуального елементу у описі фактичних обставин;
- опису порушених норм міжнародного гуманітарного права;
- формулювання обвинувачення, визнаного судом доведеним;
- правова кваліфікація діяння;
- докази на підтвердження встановлених судом обставин;
- дотримання гарантій захисту. Цей елемент указаний останнім не через применшення його важливості, а лише тому, що він є спеціальним, оскільки вироки за ст. 438 КК України ухвалюються не лише у спеціальному судовому провадженні.

Список використаних джерел:

1. Настільна книга судді з матеріалами для розгляду справ про міжнародні злочини, URL: https://nsj.gov.ua/files/1687510022%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%96%20%D0%97%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8%20%D0%9D%D0%B0%D1%81%D1%82%D1%96%D0%BB%D1%8C%D0%BD%D0%B0%20%D0%9A%D0%BD%D0%B8%D0%B3%D0%B0%20%D0%A1%D1%83%D0%B4%D0%B4%D1%96.pdf (дата звернення: 10.06.2024)
2. Главюк І.В. Дослідження: вироки за ст. 438 КК України: порушення законів та звичаїв війни (з 24 лютого 2022 року). URL: https://www.hsa.org.ua/lectors/glovyuk-iryna/articles/doslidzennia-viroki-za-st-438-kk-ukrayini-porusennia-zakoniv-ta-zvicayiv-viini-z-24-liutogo-2022-roku. (дата звернення: 10.06.2024)
3. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/114340568. (дата звернення: 10.06.2024)
4. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/114705152. (дата звернення: 10.06.2024)
5. ЄДРСР: URL: https://reyestr.court.gov.ua/Review/114511607. (дата звернення: 10.06.2024)
6. ЄДРСР: URL: https://reyestr.court.gov.ua/Review/115421876. (дата звернення: 10.06.2024)
7. Главюк І.В., Тетерятник Г.К. Контекстуальні елементи у провадженнях щодо воєнних злочинів: предмет доказування sui generis. Юридичний науковий електронний журнал. 2022. № 6. С. 394–398. DOI https://doi.org/10.32782/2524–0374/2022–6/87
8. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/111986970. (дата звернення: 10.06.2024)
9. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/111894270. (дата звернення: 10.06.2024)
10. Пашковський М.І. Кримінально-правова кваліфікація за ст. 438 КК України: до питання

про серйозність порушення законів і звичаїв війни. Кримінальне право України перед викликами сучасності і майбуття: яким воно є і яким йому бути?: Матеріали міжнар. наук. конф. м. Харків, 21–22 жовт. 2022 р., Харків, 2022. С. 120–126.

11. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/108861126. (дата звернення: 10.06.2024)

12. Головюк І.В. Чи є посилання на Римський Статут МКС у вироку елементом формулювання обвинувачення / правової кваліфікації? Теоретико-прикладні проблеми кримінального процесу та криміналістики в умовах воєнного стану: тези доп. Міжнарод. наук.– практ. конф. (м. Кам'янець-Подільський, 24 листоп. 2023 р.) Кам'янець-Подільський: ХНУВС, 2023. С. 96–100.

13. Кваша О., Андрусяк Г. Кримінальна відповідальність командирів за віддання злочинних наказів про порушення законів і звичаїв війни у контексті війни Росії проти України. Слово Національної школи суддів України. 2023. № 3(44). С. 110–125. DOI 10.37566/2707–6849–2023–3(44)-10

14. Пашковський М.І. Командна відповідальність для російських командирів на підставі ст. 438 КК України та ст. ст. 86, 87 Першого Додаткового протоколу до Женевських конвенцій: перспективи використання хорватського досвіду. DOI https://doi.org/10.30525/978–9934–26–324–8–26. (дата звернення: 10.06.2024)

15. Вознюк А.А. Командна відповідальність: проблеми притягнення до кримінальної відповідальності та перспективи удосконалення кримінального законодавства України. Ретроспектива військової агресії рф в Україні: злочини проти миру, безпеки людства та міжнародного правопорядку в сучасному вимірі: матеріали міжнародного науково-практичного круглого столу (Київ, 22–23 черв. 2023 р.). Київ: Алерта, 2023. С. 64–72.

16. Яковлєв Андрій, Тимочко Максим, Руденко Владислав. Командна відповідальність за лаштунками Кримінального кодексу. URL: https://justtalk.com.ua/post/komandna-vidpovidalnist-za-lashtunkami-kriminalnogo-kodeksu

17. ЄДРСР. URL: https://reyestr.court.gov.ua/Review/110409601. (дата звернення: 10.06.2024)

ВИКОРИСТАННЯ СТЕРЕОТИПНИХ УЯВЛЕННЬ ПРО ГЕНДЕРНУ РІВНІСТЬ ЯК ЕЛЕМЕНТ ВПЛИВУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ УКРАЇНИ

Вадим ГРОХОЛЬСЬКИЙ
кандидат юридичних наук, доцент
провідний науковий співробітник
Національного юридичного університету
імені Ярослава Мудрого

Згідно частини 4 статті 3 Закону України «Про національну безпеку України», державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями. [1] Таким чином, інформаційна безпека нашої держави, закріплена як складова національної безпеки України. Відповідно Стратегії інформаційної безпеки, затвердженої Указом Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року, інформаційна безпека України визначається, як складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, викори-

стання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. [2]

В наш час, інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації.

Під впливом інформаційних атак може цілеспрямовано змінюватися кругозір та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, тому на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах. [3]

В умовах війни в Україні, російський агресор, дуже часто використовує засоби інформаційного впливу для здійсненням інформаційно-психологічних операцій. Дуже поширеним заходом, виправдування свої агресивних дій є використання інформації, де акцентується увага на стереотипних уявленнях, щодо євроінтеграційних цінностей України в цілому та гендерної рівності зокрема, які транслюються медіа та окремими лідерами суспільної думки.

Розберемо, які саме стереотипні уяви частіше за все використовує ворог. По-перше, гендерна рівність руйнує родини й пришвидшує депопуляцію українців. Це твердження, на жаль, культивують не лише необізнані люди, але й політики та державні діячі. Насправді, гендерна рівність –це досягнення рівних прав та можливостей між чоловіками та жінками в усіх сферах життєдіяльності. Від виховання до представництва у владі. Досягнення її потрібне, щоб соціальна, економічна, культурна та політична система нормально функціонували. Жоден її противник досі не пояснив, яким чином, наприклад, рівність на ринку праці, зменшення масштабів домашнього насильства чи подолання сексизму негативно вплине на традиційну родину. [4]

По-друге, термін «гендер» необхідно прибрати із законодавства й замінити його словом «стать», адже це крок до пропаганди одностатевих стосунків. Щоб розвінчати цей міф необхідно перш за все зрозуміти, що означає поняття «гендер». Гендер (від англ. gender–рід) –соціокультурна, символічна конструкція статі, що покликана визначати конкретний асоціативний зв'язок, забезпечувати повноцінну комунікацію та підтримувати соціальний порядок [5, с. 45]. Гендер стосується стилю життя та способу мислення, ролей та відносин жінок і чоловіків, набутих ними як особистостями в процесі соціалізації. Все це визначається соціальним, політичним, економічним і культурним контекстами буття й фіксує уявлення про жінку та чоловіка залежно від їх статі. Тому ініціативи деяких політиків замінити термін «гендер» на термін «стать» виглядають щонайменше дивними. Вони не є взаємозамінними, адже стосуються різних речей. Якщо стать це незмінна біологічна характеристика набута при народженні, то гендер поняття змінне у часі. [4]

По-третє, гендерно чутлива політика загрожує духовності. На цьому твердженні багато спекулюють. Незрозуміло, що критики розуміють під духовністю та як можна виміряти її рівень? Україна –духовна чи ні? В російській федерації міфічна духовність стала основою так званих «духовних скреп». Результатом є, наприклад, декриміналізація домашнього насильства. [4]

Завдяки використанню вказаних стереотипів, які вкоренилися у свідомості громадян рф, а також і деяких необізнаних прошарках українського суспільства та свідомих політичних колах України, що будуть на цьому свої популярність, реалізується програма виправдання свої імперіалістичних планів.

Засобами протидії від вказаних форм інформаційного впливу є наступні дії:

1. Проведення просвітницької роботи починаючи за середніх начальних закладів освіти, щодо гендерної політики нашої держави;

2. Створення і поширення контенту через засоби масової інформації, щодо гендерної політики України, її термінології, та правового і соціального підґрунтя реалізації вказаної політики;

3. Робота з ЛГД (лідерами громадської думки), щодо розповсюдження об'єктивної інформації по реалізації гендерної політики в українському суспільстві;

4. Виявлення зацікавлених осіб, які застосовують гендерні стереотипи для впливу на громадську думку та проведення аналізу вказаного впливу з правовою оцінкою їх діяльності.

Тільки об'єднання зусиль держави у особі її органів та громадянського суспільства, можливо подолати негативний інформаційний вплив на інформаційну безпеку України з боку держави агресора та колаборантів. Разом до ПЕРЕМОГИ!

Список використаних джерел:

1. Закон України «Про національну безпеку України» від 21 червня 2018 року, № 2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2469–19#Text (дата звернення 15.06.2024).

2. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»» 28 грудня 2021 року № 685/2021 URL: https://zakon.rada.gov.ua/laws/show/685/2021#top (дата звернення 15.06.2024).

3. Презентація «Інформаційна безпека як складова національної безпеки України» URL: https://naurok.com.ua/prezentaciya-informaciyna-bezpeka-yak-skladova-nacionalno-bezpeki-ukrani-255768.html (дата звернення 15.06.2024).

4. Суслова І.М., Голуб О.А. Гендерна рівність як цивілізаційний вибір України. URL: https://journals.uran.ua/ispss/article/view/196054/197957. (дата звернення 15.06.2024).

5. Словник гендерних термінів / укладач З.В. Шевченко.– Черкаси: Видавець Чабаненко Ю., 2016.–336 с.

ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТАРІЮ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ВЛАСНОСТІ

Олексій ДЕРЕВЯГІН
кандидат юридичних наук, старший науковий співробітник,
професор кафедри оперативно-розшукової діяльності
та розкриття злочинів факультету № 2
Харківського національного університету внутрішніх справ

Кримінальні правопорушення проти власності мають складну природу та можуть включати різноманітні аспекти: від технічних деталей до психологічних характеристик правопорушників. Для швидкого розкриття таких кримінальних протиправностей необхідно використовувати комплексний підхід, який включає аналіз технічних аспектів вчинення злочину, вивчення мотивацій та психології правопорушників, а також виявлення засобів комунікації та місць їхнього знаходження тощо.

В епоху цифрових технологій, коли інформація стає доступною з різних джерел, використання OSINT (Open Source Intelligence) інструментарію набуває важливого значення при розслідуванні кримінальних правопорушень. Слід зазначити, що (OSINT) – це процес збору, аналізу і використання інформації, яка відкрито доступна. Ця інформація може бути отримана з різних джерел, таких як вебсайти, соціальні мережі, публічні бази даних, новинні ресурси, блоги тощо. Основна мета OSINT – зібрати релевантну інформацію для подальшого аналізу і прийняття рішень. Цей підхід застосовується в різних сферах, включаючи правоохоронну діяльність, розвідку, бізнес-аналітику, кібербезпеку та ін. В сучасних умовах, коли велика

кількість інформації публікується онлайн, OSINT стає важливим інструментом для здійснення різних видів аналізу та досліджень, у тому числі і при розслідуванні кримінальних правопорушень проти власності [1].

Розкриття кримінальних правопорушень проти власності, за допомогою відкритих джерел (OSINT), включає в себе процес збору, аналізу та використання публічно доступної інформації. Відкриті джерела включають в себе вебсайти, соціальні мережі, форуми, блоги та інші онлайн-ресурси, де правопорушники можуть залишити сліди своєї діяльності. Завдяки використанню OSINT правоохоронці збирають важливі дані про з зловмисників, способи і місця реалізації викраденого майна, використані інтернет ресурси та інші характеристики протиправної діяльності. Це також допомагає встановити шаблони поведінки правопорушників у віртуальному просторі (середовищі), їх мету та способи ухилення від виявлення. Крім того, аналіз відкритих джерел розкриває можливі зв'язки між різними правопорушниками у віртуальному просторі (середовищі), а також надає інформацію для подальшого використання в розслідуванні та судових процесах [2].

Один із основних аспектів застосування OSINT при розслідуванні кримінальних правопорушень проти власності, є зіставлення різних джерел інформації, що дозволяє побудувати повну картину кримінальної активності зловмисників. Це сприяє виявленню закономірностей, які використовують для вивчення їхньої поведінки та ідентифікації.

Засоби OSINT залучають широку групу фахівців, включаючи правоохоронців, кібераналітиків та спеціалістів з кібербезпеки, до спільної роботи над виявленням та розслідуванням незаконної діяльності у кіберпросторі.

Використання OSINT для розслідування кримінальних правопорушень проти власності, передбачає кілька етапів, які спрямовані на збір, аналіз та використання публічно доступної інформації. До основних етапів цього процесу слід віднести:

1. *Збір інформації*. У процесі розслідування такого роду правопорушень будуть корисними всі раніше здобуті знання та навички, які в тій чи іншій мірі дозволяють користуватися відкритими джерелами задля, наприклад, ідентифікації місцевості чи осіб, які зображені на фото чи фігурують у відео. Власне, розрізняють пасивні та активні методи проведення розслідування кримінальних правопорушень проти власності з допомогою відкритих джерел.

Пасивні методи дозволяють отримувати загальну інформацію про об'єкт. Вона збирається вручну або за допомогою спеціальних сервісів та інструментів, що спрощують збір, систематизацію та аналіз даних. Наприклад, програм для парсингу сайтів. До пасивних методів можна віднести:

- збирання інформації (у тому числі за фотографіями) з відкритих пошукових систем;
- аналіз активності користувача в соціальних мережах і блогах, на форумах, інших віртуальних платформах;
- пошук відкритих персональних даних користувачів у соціальних мережах, месенджерах;
- перегляд збережених копій сайтів у пошукових системах, інтернет-архіві;
- отримання геолокаційних даних за допомогою загальнодоступних ресурсів, таких як Google Maps.

Активні методи. Такі методи мають на увазі безпосередній вплив аналітика на досліджуваний об'єкт, використання спеціалізованих засобів отримання даних або здійснення дій, що вимагають певних зусиль, наприклад:

- збір даних на закритих ресурсах, доступ до яких можливий лише за передплатою;
- застосування спеціалізованих сервісів та програм, які активно впливають на досліджуваний об'єкт (наприклад, автоматично реєструються на сайті);
- використання сервісів, що сканують програми, файли чи сайти на наявність шкідливого коду;
- створення підроблених вебресурсів, каналів у месенджерах, які збирають дані користувачів, конфіденційні чи секретні відомості.

У логіці OSINT пасивні методи, спрямовані на збір загальної інформації з доступних джерел, передують застосуванню активних способів, призначених для збору конкретних даних про об'єкт [3; 4, с. 164–165].

2. *Фільтрація та сортування*. Зібрану інформацію необхідно відфільтрувати та сортувати залежно від релевантності та значущості. Важливо виділити ключові дані, які можуть вказувати на кримінальну протиправну діяльність.

3. *Аналіз інформації.* На цьому етапі проводиться детальний аналіз зібраної інформації. Встановлюються зв'язки між різними джерелами та особами, розглядаються можливі закономірності.

4. *Крос-перевірка і підтвердження*. Для забезпечення точності та достовірності інформації проводиться крос-перевірка даних з декількох джерел. Це допомагає підтвердити отримані дані та визначити, які з них є вірогідними.

5. *Створення аналітичних звітів.* На основі аналізу формується аналітичний звіт, який містить важливу інформацію, яка становить оперативний інтерес, залучення сторін, можливі наслідки та рекомендації для подальших дій.

6. *Спільна робота та співпраця*. Важливо залучити до розслідування спеціалістів з різних областей, які можуть надати цінний внесок у виявленні та аналізі кримінальних правопорушень проти власності [5, с. 99].

Так, в контексті використання наявного інструментарію підрозділів кримінального аналізу підкреслимо можливість застосування геопросторового методу аналітичного дослідження. Така аналітична діяльність надає змогу забезпечити оперативність розкриття кримінальних правопорушень проти власності. Наприклад, маючи відомості щодо місця вчинення «вуличного» кримінально-протиправного діяння, такого як грабіж або розбій, користуючись наявними обліками, аналізу кримінальних проваджень щодо придбання, отримання, зберігання чи збуту майна, одержаного кримінально протиправним шляхом, аналітик має змогу встановити всі наявні місця ймовірного подальшого збуту викраденого майна, шляхом здійснення аналітичного дослідження локації в якій таке діяння було вчинено, як наслідок – можливість швидкого відпрацювання таких місць.

Встановивши місце збуту викраденого майна, яке стало предметом кримінально-протиправного посягання перед кримінальним аналітиком постає можливість здійснення аналітичного дослідження щодо наявності камер відеоспостереження в локації місця реалізації викраденого майна – з метою отримання або уточнення відомостей щодо візуальних ознак зловмисника та відстеження його шляхів переміщення [6, с. 38–39].

Окрім цього, як навчальний інструмент та практичний посібник для правоохоронців з використання відкритих цифрових даних для проведення розслідувань кримінальних правопорушень проти власності, може бути використаний практичний посібник Протокол Берклі [7; 8]. Документ містить стандарти знаходження, збирання, зберігання, перевірки та аналізу контенту із соцмереж та інших відкритих джерел; міжнародні стандарти для проведення онлайн-розслідування; керівництво про методи та процедури для збирання, аналізу та зберігання цифрової інформації з дотриманням професійних, правових та етичних принципів. Також у посібнику викладено заходи, які слідчі можуть вжити в Інтернеті, щоб забезпечити фізичний та психосоціальний захист самих себе та інших людей, включаючи свідків, постраждалих, громадян, активістів та журналістів [9; 10].

Окрім зазначеного, потужними інструментами, які можуть бути використані для розслідування кримінальних правопорушень проти власності, через аналіз відкритих джерел інформації OSINT є:

1) Maltego – це універсальна розвідувальна платформа з відкритим кодом, яка може спростити та прискорити розслідування. Він надає доступ до 58 джерел даних і можливості ручного завантаження, а також баз даних до 1 мільйона об'єктів, щоб допомогти вам проводити кращий аналіз. Його потужні інструменти візуалізації також дозволяють вибирати з різних макетів, таких як блоки, ієрархічні чи кругові графіки з вагами та примітками для подальшого вдосконалення;

2) Spiderfoot – це інструмент OSINT-розвідки з відкритим вихідним кодом із різноманітними функціями, включаючи можливість отримувати та аналізувати IP-адреси, діапазони CIDR, домени та субдомени, ASN, адреси електронної пошти, номери телефонів, імена та імена користувачів, адреси BTC тощо. Пропонуючи як інтерфейс командного рядка, так і вбудований веб-сервер із зручним графічним інтерфейсом користувача, який доступний на GitHub, Spiderfoot може похвалитися понад 200 модулями, які можна використовувати для виконання найповніших дій і розкриття ключових деталей про будь-яка мета;

3) OSINT Framework – ресурс для збору розвідувальних даних із відкритим кодом. У ньому є все: від джерел даних до корисних посилань на ефективні інструменти, що робить його набагато легшим, ніж намагатися окремо досліджувати кожну програму та інструмент. Цей каталог також містить опції для операційних систем поза межами Linux, надаючи рішення для всіх напрямків. Єдиною проблемою може бути розробка ефективної стратегії пошуку, яка звужує результати, такі як реєстрація транспортного засобу чи адреси електронної пошти, але з такими організованими ресурсами це стає більшим активом, ніж будь-коли.

4) Recon-ng – це потужний інструмент, який використовується для пошуку інформації, пов'язаної з доменами веб-сайтів. Використовуючи Recon-ng, аналітики можуть визначати веб-уразливості, включаючи пошук GeoIP, пошук DNS і сканування портів. Це надзвичайно корисно для пошуку конфіденційних файлів, таких як robots.txt, пошуку прихованих субдоменів, пошуку помилок SQL і отримання інформації CMS компанії або WHOIS;

5) Aircrack-ng – це потужний і комплексний інструмент для перевірки проникнення в безпеку, який використовується фахівцями з цифрової безпеки для перевірки безпеки бездротових мереж. Інструмент дозволяє користувачам збирати інформацію, пов'язану з моніторингом пакетів, включаючи захоплення кадрів і збір WEP IV разом із положенням точок доступу, якщо додано GPS;

6) BuiltWith – це неймовірно потужний детектив для веб-сайтів, який дозволяє користувачам дізнаватися про технічний стек, фреймворки, плагіни та іншу інформацію, яка підтримує популярні веб-сайти;

7) Metagoofil – це безкоштовно доступний інструмент на GitHub, який спеціалізується на вилученні метаданих із різноманітних загальнодоступних документів, зокрема.pdf,.doc,.ppt і.xls. Будучи неймовірно потужною пошуковою системою, вона здатна знаходити такі корисні дані, як імена користувачів і справжні імена, пов'язані з певними загальнодоступними документами, а також інформацію про сервер і шлях до цих документів;

8) Sherlock – програма на Python, яка на сайтах соціальних мереж перевіряє, чи зареєстрований там користувач із вказаним іменем.

9) Photo Sherlock (інша версія цієї програми) – шукає в Інтернеті фото з камери чи галереї. Дану програму можна використовувати, щоб знайти інформацію про зображення в Інтернеті, наприклад, щоб перевірити кому дійсно належить фото з соціальної мережі (перевірка на фейк) [11].

Отже, підсумовуючи, варто зауважити, що засоби розслідування та колекції ресурсів OSINT революціонізують спосіб збирання, аналізу та використання відкритої інформації. Вони допомагають зробити цей процес більш ефективним, точним та систематичним. З ними здатність здобувати інсайти, розуміти ситуацію та приймати обґрунтовані рішення в процесі розслідування кримінальних правопорушень проти власності стає безмежною. Засоби розслідування та колекції ресурсів OSINT глибоко проникають у світ відкритої інформації, відкриваючи перед поліціянтами безмежні можливості. Ці інструменти не лише полегшують процес збору та аналізу даних, а й допомагають виявляти важливі взаємозв'язки та шаблони, які можуть залишитися непоміченими під час огляду місця події або при проведенні первинних слідчо-розшукових дій. Таким чином, з урахуванням дії правового режиму воєнного стану в Україні правоохоронним органам нашої країни, зокрема працівникам Національної поліції України, необхідно опановувати метод OSINT та вдосконалювати навички його використання під час досудового розслідування кримінальних правопорушень, зокрема проти власності.

Список використаних джерел:

1. OSINT: технологія збору та аналізу даних з відкритих джерел. 2022. URL: https://softlist.com.ua/articles/osint-tekhnologiya-sbora-i-analiza-dannyh-iz-otkrytyh-istochnikov/ (дата звернення: 16.06.2024).

2. Кисельов А. Досвід використання підрозділами Національної поліції технологій «OSINT» у протидії кримінальним правопорушенням. *Міжнародна та національна безпека: теоретичні і прикладні аспекти*: матеріали VI Міжнар. наук.– практ. конф. (м. Дніпро, 11 березня 2022 р.). – Дніпро: ДДУВС, 2022. С. 318–319.

3. Як OSINT впливає на війну в Україні? Itedu: вебсайт. URL: https://itedu.center/ua/blog/articles/osint/ (дата звернення: 16.06.2024).

4. OSINT при розслідуванні кримінальних правопорушень: підручник / О.О. Торбас. – Одеса: Видавництво «Юридика», 2024. – 180 с.

5. Організація розкриття шахрайств, учинених в кіберпросторі: монографія / Шевчишен А.В., Романов М.Ю., Волобоєв А.О., Лунгол О.М., Габорець О.А., Головкін С.В.; за заг. ред. С.С. Вітвіцького. Київ: Алерта, 2023. 200 с.

6. Руденко А., Халявка І., Кисельов А. Використання можливостей кримінального аналізу в процесі викриття кримінальних правопорушень проти власності. *UNIVERSUM | Березень 2024*, 6, 2024. С. 36–41. URL: https://archive.liga.science/index.php/universum/article/view/819 (дата звернення: 16.06.2024).

7. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних / Управлін. Верховн. комісара ООН з прав людини та Центру з прав людини Каліфорн. ун-ту в Берклі, Юрид. шк., 2022. 119 с. URL: https://www.law.berkeley.edu/wpcontent/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 16.06.2024).

8. Деревягін О.О. Напрями підвищення ефективності досудового розслідування кримінальних проваджень в умовах воєнного стану. *Законодавчі аспекти протидії особливо небезпечним злочинам в Україні:* матеріали міжнар. наук.– практ. круг. столу (м. Київ, 14–15 берез. 2024 р.). Київ: Алерта, 2024. С. 242–244.

9. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник. Нью-Йорк і Женева, 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 16.06.2024).

10. Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. Юрфем.UA. 2022. URL: https://jurfem.com.ua/protokol-berkli-schodo-rozsliduvannia-iz-vykorystannyam-zyfrovych-danych/ (дата звернення: 16.06.2024).

11. 10 найкращих інструментів Open Source Intelligence (OSINT): вебсайт. URL: https://www.unite.ai/uk/best-open-source-intelligence-osint-tools/ (дата звернення: 16.06.2024).

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО СУДОВО-ЕКСПЕРТНИХ УСТАНОВ ЯК НАПРЯМ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Андрій ДЕРЕЧА
судовий експерт
Науково-дослідного центру судової експертизи
у сфері інформаційних технологій та інтелектуальної власності
Міністерства юстиції України
Руслан МІРОШНИК
судовий експерт
Науково-дослідного центру судової експертизи
у сфері інформаційних технологій та інтелектуальної власності
Міністерства юстиції України

Питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо [1].

Широкомасштабна військова агресія російської федерації в Україні зумовила необхідність подолання нових викликів воєнного часу, у тому числі, забезпечення інформаційної безпеки держави. У статті 107 Конституції України зазначено, що Рада національної безпеки і оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України, яка координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони [2].

Крім того, Указом Президента України від 14.09.2020 № 392/2020 затверджено Стратегію національної безпеки України «Безпека людини – безпека країни», де визначено пріоритети національних інтересів України та забезпечення національної безпеки, цілі та основні напрями державної політики у сфері національної безпеки; поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов; основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки; напрями та завдання реформування й розвитку сектору безпеки і оборони; ресурси, необхідні для реалізації Стратегії. Відповідно до пункту 4 розділу І цього Указу, стратегія національної безпеки України ґрунтується на таких основних засадах:

– стримування – розвиток оборонних і безпекових спроможностей для унеможливлення збройної агресії проти України;
– стійкість – здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема шляхом мінімізації зовнішніх і внутрішніх уразливостей;
– взаємодія – розвиток стратегічних відносин із ключовими іноземними партнерами, насамперед з Європейським Союзом і НАТО та їх державами- членами, Сполученими Штатами Америки, прагматичне співробітництво з іншими державами та міжнародними організаціями на основі національних інтересів України.

Україна поступово накопичує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Питання дезорганізації роботи інформаційних систем і мереж, протиправної діяльності осіб в умовах активізації кібервтручань є дуже актуальним особливо зараз, під час збройної агресії Росії проти України, у зв’язку з цим, необхідно виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки.

Важливу роль щодо забезпечення інформаційної безпеки відіграють судові експерти судово-експертних установ, зокрема, науково-дослідних установ судових експертиз Міністерства юстиції України.

Одним із завдань судової експертизи електронних комунікацій є дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій, визначення характеристик та параметрів телекомунікаційних систем та засобів, встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах, встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій тощо.

При цьому експерт вирішує такі питання: «Які технічні характеристики (параметри) має телекомунікаційний засіб (система)?», «Чи мав місце факт доступу до телекомунікаційної системи та в який спосіб?», «Чи мало місце використання ресурсів та інформації в телекомунікаційній системі та в який спосіб?», «Чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб?», «Чи є ознаки втручання в роботу телекомунікаційної системи?», «Чи могли апаратні засоби об'єднуватись у телекомунікаційну мережу та за якими ознаками?», «Які шляхи маршрутизації даних у телекомунікаційній системі?», «Чи можливо використання телекомунікаційного засобу (обладнання) для вказаних цілей?» [4].

Глобальне поширення інформаційних мереж, передусім Інтернету, зумовлює актуалізацію вищевказаної глобальної проблематики, що є важливим під час виявлення кіберзагроз, що сприяє розгляду фахівцями судово- експертних установ України та зарубіжжя, розвитку міжнародного співробітництва у галузі судової експертизи.

На цей час у світі практично не існує держав, які б, здійснюючи свою внутрішню і зовнішню політику, не співпрацювали з іншими державами через відповідні міжнародні організації, міністерства, відомства та інші центральні органи державної влади, державні установи, громадські організації та ін. За останні роки помітно зросла роль міжнародного співробітництва, що пов'язано з процесами інтернаціоналізації та глобалізації всіх сфер людської діяльності, стрімким розвитком засобів комунікації, розвитком міжнародних наукових зв'язків, активізацією міжнародної транснаціональної організованої злочинності у сфері інформаційної безпеки, боротьби зі злочинами та іншими правопорушеннями в інформаційній сфері міжнародного тероризму, воєнних злочинів тощо.

З метою швидкого, об'єктивного та всебічного розкриття та розслідування злочинів, необхідно істотно підвищити вимоги до оперативності та ефективності роботи правоохоронних органів, судів, чия діяльність, у свою чергу, багато в чому залежить від якісної роботи судових експертів.

На розвиток судово-експертної діяльності та розширення можливостей судових експертиз позитивно впливає здійснення міжнародних контактів між судово-експертними установами: взаємне інформування за напрямами досліджень, організація спільних міжнародних науково-практичних конференцій, симпозіумів, семінарів, «круглих столів», а також стажувань фахівців з метою обміну досвідом роботи, телекомунікаційні зв'язки з питань судової експертизи, ознайомлення зі структурою, організацією діяльності та новітніми методиками проведення експертиз, що дозволяє фахівцям постійно перебувати в курсі останніх досягнень науки та використовувати досвід своїх колег з інших країн.

Останнім часом спостерігається зростання кількості укладених міжнародних договорів між міністерствами юстиції різних держав, у тому числі, в галузі судово-експертної діяльності, що обумовлено прагненням міжнародного судово-експертного товариства розширити можливості обміну науковою та практичною інформацією з питань судової експертизи. Активізація обміну науковими досягненнями в галузі судової експертизи викликана постійним прагненням судових експертів використовувати при проведенні судових експертиз ефективніші сучасні засоби, методи та методики досліджень.

Сучасний стан і перспективи розвитку судової експертизи відображають, насамперед, потреби судово-слідчої практики, зумовлені, в основному, характером злочинності, боротьба з якою вимагає високої кваліфікації та досвіду судових експертів, умов їх праці, науково-методичного, інформаційного та інструментального програмного забезпечення, а також удоскона-

лення різних форм міжнародних зв'язків, рівня професіоналізму, розвитку інституту судової експертизи. Реалізація потенційних можливостей судово-експертних установ прямо залежить від подальшого розвитку міжнародного співробітництва судово-експертних установ України та міжнародних організацій для забезпечення якості досліджень, застосування передових технологій та досвіду, вирішення стратегічних завдань, що виникають у нових соціально-політичних і економічних умовах в реалізації спільних рішень, зокрема, у забезпеченні кібербезпеки.

Організація державної судово-експертної діяльності системи Міністерства юстиції має свою специфіку, обумовлену її правовими, методичними, управлінськими, матеріально-технічними, кадровими та іншими ресурсами. Так, науково-дослідні установи судових експертиз Міністерства юстиції України здійснюють свою діяльність на основі єдиних науково-методичних підходів, загальних вимог до атестації судових експертів, підготовки кадрів та підвищення їхньої кваліфікації та ін. Спостерігається постійна позитивна тенденція до розширення науково-методичної та технічної бази, впровадження та освоєння нових методик проведення судових експертиз.

Так, останнім часом працівниками судово-експертних установ освоєно низку методик проведення досліджень електронних комунікацій: «Методика комплексних досліджень комп'ютерних та електронних комунікацій, пов'язаних з виявленням фактів спотворення процесу обробки інформації та порушення правил маршрутизації в мережах електрозв'язку з використанням технології VoIP», «Методика дослідження білінгових даних операторів зв'язку по встановленню місця знаходження абонентів в певні періоди часу відносно базових станцій».

Вже стало поширеною практикою проведення судових експертиз у складі комісій експертів різних судово-експертних установ України. Така практика може мати місце також в аспекті міжнародного співробітництва фахівців різних країн, що передбачено статтями 22–24 розділу IV Закону України «Про судову експертизу», однак, така взаємодія потребує розроблення механізму організації та проведення комплексних і комісійних експертиз, процедури участі іноземних експертів у проведенні експертиз та досліджень.

Це питання за ініціативи та організаційного супроводження Мін'юсту неодноразово обговорювалося з прийняттям відповідних рекомендацій на засіданнях Координаційної ради з проблем судової експертизи при Міністерстві юстиції України, де акцентовано увагу на тому, що актуальним на цей час є необхідність залучення іноземних експертів до проведення судових експертиз в Україні, пов'язаних із розслідуванням воєнних злочинів. Зазначалося, що це також є важливим для формування належної доказової бази для майбутніх судових процесів у міжнародних судових інстанціях.

Висвітлено, що протистояння агресору спонукає до розширення співпраці, потребує консолідації зусиль державних органів, фахівців, які залучені до призначення судової експертизи, її проведення та використання її результатів, з метою пошуку дієвих шляхів підвищення ефективності судової експертизи, забезпечення відповідних суб'єктів незалежною, кваліфікованою і об'єктивною експертизою.

В даний час триває робота з активної міжнародної співпраці фахівців судово-експертних установ України та іноземних держав в галузі судової експертизи та криміналістики, проведено цілу низку заходів, що дозволяє забезпечувати стандарти якості роботи порівняно зі світовими, істотно розширює горизонти судово-експертної діяльності, сприяє сталому розвитку судової експертизи та криміналістики.

Отже, аналіз досліджуваної проблеми дозволяє виявити найбільш актуальні напрями розвитку міжнародного співробітництва, визначити основні тенденції та перспективи взаємодії судово-експертних установ в умовах сьогодення, обміну інформацією з іноземними державами та міжнародними організаціями з питань забезпечення інформаційної безпеки, боротьби зі злочинами та іншими правопорушеннями в інформаційній сфері, що здійснюється згідно з міжнародними договорами України. При цьому актуальним є якісне кадрове забезпечення судово-експертних установ відповідними фахівцями у сфері інформаційної безпеки – судовими експертами з дослідження комп'ютерної техніки та програмних продуктів, а також дослідження електронних комунікацій.

Таким чином, вдосконалення системи судово-експертних установ, підвищення ефективності їх діяльності є одним із чинників, що визначають рівень боротьби із сучасною злочинністю, зокрема, кіберзлочинністю, необхідністю забезпечення інформаційної безпеки, у зв'язку з чим необхідно вжити заходів щодо організації взаємодії різних судово-експертних установ, підвищення ефективність їх роботи, сприяння підвищення рівня науково- методичної роботи, якості судових експертиз і експертних досліджень, організації забезпечення проведення спеціальної підготовки та підвищення кваліфікації судових експертів, поновлення комп'ютерно-технічного обладнання, поліпшення матеріального забезпечення тощо.

Саме такий статус судово-експертних установ разом з оснащеністю сучасним науковим устаткуванням, надійною в науковому відношенні методичною базою, а також наявністю висококваліфікованих кадрів сформував у суспільстві, перш за все, у працівників правоохоронних органів і судів, заслужений авторитет як гарантію одержання об'єктивних і науково обґрунтованих доказів.

Вищенаведене переконливо свідчить про те, що для забезпечення інформаційної безпеки необхідним є здійснення комплексу заходів, координація діяльності державних органів з питань інформаційної безпеки, суб'єктів забезпечення інформаційної безпеки, запровадження дієвих механізмів виявлення та фіксації правопорушень проти інформаційної безпеки держави, створення сприятливих умов для підвищення рівня професійної підготовки фахівців, зокрема, судових експертів, консолідація зусиль фахівців судово-експертних установ України та зарубіжжя.

Список використаних джерел:

1. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України // Інформація і право. № 3(15). 2015. С. 36–42.

2. Конституція України (прийнята на п'ятій сесії Верховної Ради України, 28.06.1996, із змінами) // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

3. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 17.06.2024).

4. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 08.10.1998 № 53/5. URL: https://ips.ligazakon.net/document/REG3145 (дата звернення: 17.06.2024).

5. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII. URL: https://ips.ligazakon.net/document/t403800?ed=2003_04_03 (дата звернення: 17.06.2024).

КІБЕРВІЙНА, ЯК ОБ'ЄКТ, ЩО ПОТРЕБУЄ МІЖНАРОДНОГО ВРЕГУЛЮВАННЯ

Артем КОГУТ
старший викладач
Національного юридичного університету
імені Ярослава Мудрого

Термін «кібервійна» застосовується вже більше 15 років. Під ним розуміють загрозу кіберпростору, яка за своєю суттю та наслідками може бути прирівняна до військового протистояння між державами, що виражається однієї держави з проникнення у комп'ютери або мережі іншої держави для досягнення власних цілей із заподіяння шкоди або руйнування. Деякі науковці визначають кібервійну як протистояння у мережі Інтернет, направлене, в першу чергу, на виведення з ладу комп'ютерних систем державних органів країни-супротивника, а також

інформаційних систем її критичної інфраструктури. Також існує підхід, згідно з яким до елементів кібервійни відносять масовані інформаційні впливи, як елементу міждержавного протистояння, що проектується у кіберпросторі (так звана «війна фейків»).

Активно про кібервійну заговорили після потужних кібератак на Естонію та Грузію, які були здійснені у 2007 та 2008 роках відповідно. Вказані атаки були проведені шляхом використання великої кількості «DoS-зомбі», об'єднаних в одну мережу під єдиним керуванням. При цьому, у Грузії під час вказаної атаки було оголошено воєнний стан та йшли бойові дії, що і надає повне право віднести конкретну атаку до складових кібервійни. При цьому, вже у 2009 році дослідники безпеки з Greylogic знайшли ряд підтверджень ключової ролі російських органів розвідки та безпеки в координації вказаних атак.

Першим же повноцінним полігоном кібервійни, нажаль, стала Україна. Так, ще напередодні повномасштабного вторгнення в Україну, починаючи з січня 2022 року росія розпочала атаки на українські сайти державного та банківського сегменту, які на той момент були найбільшими (та найдорожчими за обсягами наслідків) в історії України.

У подальшому, в ході війни вчинялися (та вчиняються) різноманітні атаки як з боку ворога, так і з боку кіберзахисників України. Найвідомішою на сьогодні атакою на Україну є напад на потужності оператору мобільного зв'язку «Київстар», в результаті якого було виведено з ладу послуги, що надавались всією територією країни, а також знищено бази даних оператору. Що суттєво впливає на Національну безпеку України, частиною якої є безпека кіберпростору. [1]

Враховуючи те, що фактично всі сфери сьогоднішнього життя пов'язані з комп'ютерами та мережами, кібервійна має неосяжне поле для розгортання. І атаки на сайти, які несуть фінансові, іміджеві втрати та створюють певні незручності,– це лише «верхівка айсбергу». На глибині криється багато загроз, починаючи від шпигунства за супротивником, закінчуючи фізичним виведенням з ладу підприємств, в тому числі які нестимуть загрозу хімічного забруднення, ядерної катастрофи тощо.

Таким чином, оскільки кібервійна може нести загрозу існуванню людства, а світовий порядок передбачає спільне вироблення механізмів колективного вирішення глобальних проблем людства, то повинні існувати певні правила та обмеження при веденні вказаного виду війн. Вказана проблема вже неодноразово підіймалася, в тому числі і на найвищому рівні. Так, Генеральний секретар Організації Об'єднаних націй Антоніу Гутерреш ще у 2018 році на Мюнхенській конференції зазначив, що світ повинен почати обговорення міжнародно-правові рамки ведення кібернетичної війни, оскільки взаємні удари у кіберпросторі стали реальністю.

Усе викладене свідчить про те, що світ стоїть на порозі глобального врегулювання до рамок ведення війни у кіберпросторі, а український досвід може стати підґрунтям для створення міжнародних законодавчих рішень.

Список використаних джерел:

1. Закон України «Про національну безпеку України» від 21 червня 2018 року, № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469–19#Text. дата звернення: 17.06.2024).

КОНЦЕПЦІЯ «ONE VOICE» У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В ПЕРІОД ВІЙНИ

Наталія КУДРЯВЦЕВА
юрист

Про концепцію «one voice» йде мова, коли порушується питання антикризової діяльності підприємства. Дану модель пропонується розглядати як технологію донесення головних повідомлень для досягнення конкретних цілей, а також для успішної розбудови проєктів та досягнення завдань, що проявляється в тому числі і через системне планування роботи [1, с. 51]. При цьому, уведення технологічно та методологічно єдиних засад оприлюднення інформації за результатами діяльності прийнято вважати одними із основних функцій інформаційної політики підприємства [2, с. 67].

Цілком зрозуміло, що єдина політика комунікаційної діяльності є обовязковою передумовою успішного існування як підприємства, так і держави в цілому. Створення платформ для посилення комунікації всередині спільнот практикується, для прикладу, в окремих сферах з питань охорони здоровя [3]. На таких тематичних майданчиках для спільнот доступні розділи з опитуваннями та відеозверненнями, де учасники можуть підіймати актуальні проблеми й запропонувати бачення для їх вирішення. Модель «one voice» широко застосовують також представники молодіжних організацій, державного сектору при організації заходів з визначення, для прикладу, ідентичності української молоді [4]. Крім того, на державному рівні Єдину інформаційну систему визначено в соціальній сфері, про яку постановою Кабінету Міністрів України від 14.04.2021 № 404 затверджено окреме Положення [5].

Водночас під час війни особливу важливість становить питання єдності державної політики в інформаційній сфері. Якщо у 2017 році на веб-сайті Радіо Свободи зазначалося, що відомої прес-службам всього світу «One Voice Strategy» (стратегії одного голосу) в антикризовій діяльності держави у нас просто не існує, а владі рекомендувалося створити єдиний центр формування стратегічного наративу [6], то у 2021 році для підтримки стратегічних державних комунікацій був створений такий Центр стратегічних комунікацій та інформаційної безпеки. Даний Центр діє досі та активно сприяє формуванню єдиної державної позиції – «one voice policy» щодо ключових процесів в Україні шляхом проведення щорічних форумів, інформаційних кампаній для внутрішньої та зовнішньої аудиторії, організації заходів співпраці з громадським суспільством тощо. Також Центром створено та розіслано щоденний месседж-бокс «Основні позиції інформаційного реагування», принципом якого є пояснення складних речей простими словами. Матеріали месседж-боксу відповідають державній політиці «єдиного голосу», в його основу покладені офіційні повідомлення, а до верифікації залучені представники МКІП, МЗС та МО України [7].

З огляду на особливості війни в Україні, Указом Президента України від 19 березня 2022 року [8] було передбачено реалізацію «єдиної інформаційної політики в умовах воєнного стану» та обєднано телеканали, уніфіковано їх програми. При цьому, з початку повномасштабного російського вторгнення державою дотримується принцип «one voice policy», коли всі українські журналісти говорять про війну єдиним голосом. Голос із позиції національних інтересів України [9].

Нещодавно під час одного із Форумів комунікаційників, що цьогоріч проходив з нагоди створення комунікаційних підрозділів системи МВС, було публічно заявлено про те, що державним органам в цілому вдалося вибудувати стратегію One Voice, яка допомагає боротися з російською пропагандою, та вдається тримати оборону на інформаційному фронті [10]. Варто сподіватися, що заявлена теза наразі є та в подальшому тривалий час буде актуальною.

Підсумовуючи, пропонуємо в інформаційній діяльності держави розглядати концепцію «one voice» в контексті узгодженої роботи не тільки ЗМІ, але й інших структурних елементів державного апарату. Так, усі без винятку органи та установи, публічні особи повинні усвідомлювати про наявність єдиного суб'єкта, що уповноважений державою надавати коментарі чи оцінку ситуації під час війни. У випадку, якщо необхідність надання пояснень стосується діяльності конкретного державного органу, здійснювати публічне обговорення чи оприлюднення відомостей з цього питання уповноважені лише посадові особи відповідного органу. За умови ідеальної моделі технологія «one voice» реалізується в контексті політики єдиної консолідованої інформаційної політики не лише усіх органів держави, але й громадян. При цьому громадяни виражають правову свідомість та проявляють розуміння до відсутності окремих видів інформації чи недоречності її публікування під час дії воєнного стану на благо захисту безпеки держави. Саме за таких умов – безумовного дотримання концепції «one voice» – може бути досягнуто значних успіхів в інформаційній війні з ворогом та забезпеченні інформаційної безпеки держави.

Список використаних джерел:

1. Лара Мудрак Комунікація і криза як громадам протистояти викликам і успішно діяти в період кризи / посібник. Київ, 2020. 107 с.

2. Гудзь О., Маковій В. Концептуальні основи формування інформаційної політики підприємств. Науковий вісник Ужгородського національного університету. 2019. Вип. 23. Ч. 1. С. 65–69.

3. One voice community – нова платформа для посилення комунікації всередині спільнот. URL: https://finance.poda.gov.ua/news181011 (дата звернення: 20.06.2024).

4. В Україні пройде наймасованіший молодіжний конгрес «Українська ідентичність та її промоція у світі» URL: https://mcip.gov.ua/ewents/ (дата звернення: 20.06.2024).

5. Про затвердження Положення про єдину інформаційну систему соціальної сфери: постанова Кабінету Міністрів України від 14.04.2021 № 404. Офіційний вісник України. 2021. № 35.

6. Криза урядових комунікацій в Україні. Про деякі причини і деякі пропозиції. URL: https://www.radiosvoboda.org/a/28437716.html (дата звернення: 20.06.2024).

7. Три роки Центру стратегічних комунікацій та інформаційної безпеки. URL: https://spravdi.gov.ua/try-roky-czentru-strategichnyh-komunikaczij-golovni-dosyagnennya-ta-plany-na-majbutnye/ (дата звернення: 20.06.2024).

8. Про рішення Ради національної безпеки і оборони України від 18.03.2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19.03.2022 № 152. Офіційний вісник України. 2022. № 68.

9. «Прямий» та «5 канал» підтримують реалізацію єдиної інформполітики воєнного часу. URL: https://interfax.com.ua (дата звернення: 20.06.2024).

10. Комунікаційний форум МВС 2.0: Стратегії та інновації на передовій інформаційної війни. URL: https://mvs.gov.ua/news (дата звернення: 20.06.2024).

ОКРЕМІ ПІДХОДИ ДО РОЗУМІННЯ КІБЕРБЕЗПЕКИ В СУЧАСНИХ УМОВАХ

Микола КУЛЕШОВ
аспірант Державної наукової установи
«Інститут інформації, безпеки і права
Національної академії правових наук України»

На думку аналітиків, які досліджують окремі питання стратегічної конкуренції у кіберпросторі, військова агресія рф проти України демонструє ставки у стратегічних змаганнях в кібер-

просторі, де росія намагається пошкодити і розірвати українські військові, урядові і цивільні мережі і все, що від них залежить. Те, що росії досі не вдалося досягти стратегічного результату в Україні за допомогою кіберзасобів не означає, що потенційно вона не може цього зробити, і не повинно відволікати увагу від проблем, створюваних для воєнних зусиль України і потенціалу суспільства загалом це робити, через кібероперації російської військової розвідки. Російські спроби завдати шкоди військовій обороні України і ускладнити цивільне життя показали обмежену корисність кібероперацій для стратегічного примусу, але не варто забувати про ресурси і рішучість, які необхідні для відбиття російських кібероперацій протягом тривалого часу [1].

Розуміючи сучасний стан та актуальність проблем у сфері телекомунікацій, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами, більшість країн світу проводять комплексні заходи щодо забезпечення національної кібербезпеки. Ці заходи пов'язані, перш за все, з розробкою та вдосконаленням нормативно-правових актів, а також створенням відомчих та державних структур, що регулюють і відповідають за забезпечення безпеки в кібернетичному просторі. Проблема забезпечення кібербезпеки є доволі важливим та складним питанням, а зневажливе ставлення держави до цього питання може призвести до непередбачуваних наслідків [2, с. 27].

Локальні системи кіберзахисту членів НАТО щоденно реєструють підозрілі дії: від спроб невисокого рівня до технологічно складних атак на мережі НАТО. Більшість їх оперативно виявляються і обробляються автоматично, але деякі з них вимагають аналізу та відповіді відповідних фахівців. Кіберкоманда з більш ніж двохсот членів постійно та цілодобово захищає мережі НАТО. Вона запобігає несанкціонованому доступу, виявляє інциденти, аналізує загрози та обмінюється з союзниками інформацією про шкідливі програми, запобігаючи витоку даних, і проводить комп'ютерну експертизу, оцінку вразливості та постінцидентні оцінки.

Виклики, пов'язані з кіберпростором та кібербезпекою, вимагають не лише простого перейменування державних організацій, відповідальних за безпеку в галузі інформаційних технологій або за безпеку у галузі комунікацій. Повсюдність сучасних комп'ютерних систем та здатність здійснювати зв'язок або взаємодіяти за допомогою різних засобів, від мобільних пристроїв до комп'ютерів, що носяться, створюють для державних та недержавних суб'єктів ряд невід'ємних уразливостей та можливі вектори атак. Використання цих уразливостей може призвести до широких наслідків для національної безпеки за допомогою таких умисних дій, як шпигунство, зниження ефективності об'єктів командування та управління, крадіжка інтелектуальної власності та чутливої інформації особистого характеру, порушення надання суттєвих послуг та функціонування критично важливої інфраструктури або заподіяння збитків економіці та промисловості [3].

Цілком погоджуючись із наведеною думкою фахівців NATO, зазначимо, що сфера кіберпростору, особливо в умовах триваючої повномасштабної збройної агресії російської федерації надає досить широкі можливості в контексті проведення воєнної, розвідувально-підривної, терористичної та інших видів діяльності, спрямованої на спричинення реальної шкоди інфраструктурним об'єктам будь-якої держави. І те, наскільки держава здатна протистояти таким загрозам та нейтралізовувати їх, в цілому визначає її потенціал до економічної, воєнної, оборонної, політичної та інформаційної стабільності.

У п. 11 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кіберпростір визначається як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Кіберпростір складається з різних підключених до мережі комп'ютерних систем та інтегрованих телекомунікаційних систем. Він став однією з характерних складових сучасного суспільства, інструментом, що забезпечує та розширює швидку комунікацію, функціонування розподілених систем командування та управління, зберігання та передачу великих масивів даних та функціонування сильно розподілених систем.

Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

На підтвердження стратегічного значення захисту найбільш важливих об'єктів держави від кіберзагроз можна навести наступні аналітичні дані. Так, розвідувальне співтовариство США у доповіді Національної Розвідувальної Ради (National Intelligence Council) наголосило таке: «В умовах несформованого глобального ландшафту, багатого сюрпризами і різкими змінами, найбільш пристосованими до використання таких можливостей будуть стійкі держави і організації, що дозволить їм адаптуватися до умов, що змінюються, витримувати вплив несподіваних несприятливих факторів і вживати заходів для швидкого відновлення. Вони будуть вкладати кошти в інфраструктуру, знання і відносини, які дозволять їм витримувати потрясіння – економічні, екологічні, соціальні або кібернетичні» [4].

Нова Стратегічна концепція оборони та безпеки країн-членів НАТО, яка була підписана під час Лісабонського саміту 19 листопада 2010 року прирівняла загрози кібератак до військових загроз, що, у свою чергу, передбачає можливість відповіді на масовані кібератаки із застосуванням кіберпідрозділів національних збройних сил. Кібератаки стали одним з найбільш небезпечних викликів безпеці країн-членів Альянсу, а забезпечення кібербезпеки визначено як пріоритет Альянсу. Доктрина НАТО «Strategic Concept NATO 2010», у свою чергу, відзначає співробітництво з країнами-партнерами у сфері розбудови системи забезпечення кібербезпеки Альянсу як ключового механізму заходів Організації Північноатлантичного договору із забезпечення кіберзахисту [5]. Враховуючи спрямованість політики нашої держави до Євроатлантичної інтеграції, необхідно враховувати керівні документи Північноатлантичного Альянсу та приводити окремі стратегії та концепції у відповідність з принципами і стандартами НАТО.

Беручи до уваги положення ч. 4 ст. 3 Закону України «Про національну безпеку України», де зазначено, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо, можемо дійти до висновку, що кібербезпека є складовою національної безпеки і оборони України.

Відповідно до п. 5 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпекою визнається захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Зазначене визначення є легальним, тобто таким, що прямо передбачено у законі.

В цілому необхідно погодитись із Л.Ю. Веселовою у тому, що проблема безпеки взагалі, інформаційної й кібербезпеки, зокрема, останніми десятиліттями є надзвичайно актуальною й поширюється настільки швидко, що певним чином неможливо зосередитись на сутності нового явища та межах його використання у контексті правового забезпечення [6, с. 56]. Разом з цим, враховуючи, що сфера кібербезпеки як складової інформаційної безпеки є досить динамічною, вважаємо проаналізувати сучасні наукові думки на предмет достатності законодавчого визначення в якості понятійного базису подальшого розгалуження системи забезпечення такої безпеки.

В рекомендації Міжнародного Союзу Електрозв'язку X.1205 МСЕ-Т «кібербезпека» визначена як набір засобів, стратегій, принципів забезпечення безпеки, заходів щодо забезпечення безпеки, керівних принципів, підходів до управління ризиками, дій, професійної підготовки, практичного досвіду, страхування і технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації і користувача [7]. Спеціалісти CISCO визначають кібербезпеку

як реалізацію заходів професійно підготовленими фахівцями щодо захисту та страхування дій, засобів, технологій, критично важливих об'єктів інфраструктури суспільства та держави від цифрових атак, які використовуються у кіберпросторі. Кібербезпека передбачає збереження та постійне вдосконалення властивостей безпеки, спрямованих проти відповідних кіберзагроз [8]. Загальними завданнями забезпечення кібербезпеки було визначено гарантування цілісності, доступності та конфіденційності інформації.

Є прибічники європейського підходу до визначення кібербезпеки також у лавах вітчизняних фахівців. Так, О.Г. Корченко О.Г. розкриває сутність кібербезпеки через призму ключових ознак цього явища. На його погляд, кібербезпекою є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційного ресурсу, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем [9, с. 7] та які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної і кіберінфраструктури [10, с. 41].

Разом з цим, у Великому тлумачному словнику української мови «кібернетичний» – стосується кібернетики; який створено, працює на основі принципів, методів кібернетики [11, с. 539]. А «безпека» – стан, коли кому-, чому-небудь ніщо не загрожує [11, с. 70], тобто відсутність небезпеки. Даючи більш широке тлумачення поняттю «безпека», В.М. Заплатинський визначає його як такі умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень [12].

Таким чином європейський підхід дещо відрізняється від вітчизняного, оскільки розглядає безпеку не як стан, а як наявність або реалізацію відповідних складових, які цей стан, за загальним задумом, мають забезпечити. В.С. Павленко відносить до основних елементів кібербезпеки наступні: безпека додатків, інформація або безпека даних, безпека мережі, відновлення після кібератак, планування кіберзахисту, операційна безпека, хмарна безпека, критична безпека інфраструктури, фізична безпека, підготовка кінцевих користувачів [13, с. 31]. Як бачимо, зазначений вчений орієнтується виключно на об'єкти безпеки, при цьому не заглиблюючись у інші складові.

Розбіжності у вживанні понять і термінів, їх неповна з'ясованість, не розмежованість за обсягом та значенням, як у наукових дослідженнях, так і у міжнародно-правових актах, свідчать про те, що осмислення основних понять, складових елементів системи забезпечення кібербезпеки критичної інфраструктури з їх багатогранними формами, стандартами та засобами ще не завершено.

Список використаних джерел:

1. НАТО і стратегічна конкуренція в кіберпросторі. [Електронний ресурс].– Режим доступу: https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html. (дата звернення: 20.06.2024)

2. Войціховський А.В.

Кібербезпека як важлива складова системи захисту національної безпеки європейських країн [Електронний ресурс] / А.В. Войціховський // Журнал східноєвропейського права.– 2018.– № 53.– С. 26–37. (дата звернення: 20.06.2024)

3. Кибербезопасность. Типовой учебный план – NATO. [Електронний ресурс].– Режим доступу: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20171004_1610-cybersecurity-curriculum-r.pdf. (дата звернення: 20.06.2024)

4. Office of the Director of National Intelligence (2017) Global trends: paradox of progress. A publication of the National Intelligence Council. NIC, avialeble at: http://www.dni.gov/nic/globaltrends (Accessed January 2021). (дата звернення: 20.06.2024)

5. Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation. Active Engagement, Modern Defence / NATO. [Online]. Available: http: //www.nato. int/lisbon2010/strategic-concept-2010-eng.pdf. Accessed on: June 21, 2019. (дата звернення: 20.06.2024)

6. Веселова Л.Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: дис. … канд. юрид. наук: 12.00.07. Одеса. 2021. 500 с.

7. Рекомендація МСЕ-Т Х.1205 від 18.04.2008 17-й ДК МСЕ-Т (2005–2008) ст. 8.

8. Что такое кибербезопасность? [Електронний ресурс]: Офіційний портал американської транснаціональної компанії Cisco https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html. (дата звернення: 20.06.2024)

9. Бурячок В.Л., Корченко О.Г., Хорошко В.О., Кудінов В.А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу // Захист інформації. 2013. Том 15, № 1.– С. 5–12.

10. Корченко О.Г., Бурячок В.Л., Гнатюк С.О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк // Ukrainian Scientific Journal of Snformation Security.– 2013. № 19. С. 40–44.

11. Великий тлумачний словник сучасної _української мови (з дод. і допов.) / Уклад, і голов, ред. В.Т. Бусел.– К.; Ірпінь: ВТФ «Перун», 2005.– 1728 с.

12. Заплатинський В.М. Логіко-детермінантні підходи до розуміння поняття «Безпека». Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини. / [редкол.: П.С. Атаманчук (відп. ред.) та ін.].– Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2012.– Випуск 5.– 336 с. С. 90–98.

13. Павленко В.С.

Сутність кібербезпеки у теорії інформаційного права [Електронний ресурс] / В.С. Павленко // Право та державне управління.– 2021.– № 2.– С. 28–33. (дата звернення: 20.06.2024)

АКТУАЛЬНІ ПОТРЕБИ УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХОДІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Дмитро МЕЛЬНИК
кандидат юридичних наук, старший дослідник,
співробітник СБУ

Глобальний кіберпростір став ареною боротьби між світовими державами-лідерами за отримання переваги у вирішенні проблем і конфліктів.

З приєднанням нашої держави до глобального кіберпростору надактуальною для України стала проблема кіберзлочинності.

В сучасних умовах це протиправне явище є реальною загрозою національній безпеці багатьох держав світу. Зокрема, кіберзлочинність загрожує непередбачуваними наслідками у зв'язку з руйнування систем управління й життєзабезпечення сучасних держави і суспільства.

Так Стратегія національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020) та Стратегія забезпечення державної безпеки (Указ Президента України від 16.02.2022 № 56/2022) серед загроз національній і державній безпеці України виділяють сучасну модель глобалізації; продовження РФ гібридної війни проти України у формі систематичних кібератак; посилення кіберзагроз для об'єктів критичної інфраструктури (ОКІ), пов'язаних з несанкціонованим втручанням у їх роботу тощо.

Вищевказаний перелік загроз національній і державній безпеці уточнюється і доповнюється у Стратегії кібербезпеки України (Указ Президента України від 26.08.2021 № 447/2021):

гібридна агресія рф проти України у кіберпросторі; розвідувально-підривна діяльність у кіберпросторі шляхом вчинення тривалих, складних і прихованих кібератак на інформаційно-комунікаційні системи (ІКС) державних органів та інших ОКІ, зорганізованих іншими державами (насамперед, рф); кіберзлочинність, що завдає шкоди інформаційним ресурсам та призводить до значних матеріальних втрат; використання кіберпростору для здійснення актів кібертероризму, надання матеріальної підтримки тероризму, вчинення злочинів, пов'язаних із незаконним обігом засобів ураження, інших небезпечних предметів і речовин.

Зазначені загрози і ризики актів кіберагресії, кіберзлочинності та кібертероризму в умовах гібридної війни РФ проти України суттєво зросли після початку повномасштабної російської військової агресії та потребують вжиття системних заходів реагування на державному та міжнародному рівнях.

Україна протягом 2022–2023 років зазнала безпрецедентної кількості кібератак на інформаційні системи та мережі ОКІ – підприємств життєзабезпечення, енергетичної, транспортної сфери, державних фінансових установ, органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій тощо.

Так у 2022 році в Україні було зафіксовано 2 194 кіберінциденти, з яких 1048 мали високий або критичний рівень [1]. Вже у 2023 році ситуація суттєво ускладнилася: за даними Держспецзв'язку кількість зареєстрованих в Україні кіберінцидентів зросла на 62,5% [2].

Наразі фахівці кібердепартаменту СБУ щомісяця фіксують понад тисячу деструктивних російських інформаційних атак на українську державу та суспільство. Мета ворожих атак – провокувати деструктивні дії населення, щоб таким чином впливати на суспільно-політичну ситуацію [3].

Комплексний характер загроз національній безпеці, пов'язаних з явищем кіберзлочинності, потребує визначення інноваційних підходів до формування системи кібербезпеки та кіберзахисту ОКІ та подальшого розвитку кіберпростору в умовах глобалізації й вільного обігу інформації [4, с. 99–100].

Водночас зростаючий рівень цифровізації української держави і суспільства зумовлює потребу постійного покращення національної кіберстійкості, удосконалення системи забезпечення кібербезпеки і протидії кіберзагрозам, насамперед кіберзлочинності.

Серед основних проблем національної стійкості, які потребують невідкладного розв'язання, Концепцією забезпечення національної системи стійкості (Указ Президента України від 27.09.2021 № 479/2021) визначено недостатній рівень розвитку системи забезпечення кібербезпеки, що не дозволяє гарантувати кіберстійкість національних інформаційних ресурсів.

Зазначений стан справ знижує ефективність виконання уповноваженими суб'єктами безпекових завдань, перешкоджає забезпеченню ефективного захисту ОКІ, що суттєво підвищує небезпечність відповідних загроз національній безпеці України. Однак варто враховувати, що кібератаки активно використовуються у сучасному кіберпросторі з протиправною метою вже не лише приватними особами, але й спецслужбами іноземних держав та підконтрольними їм групами і організаціями.

Тому для покращення протидії загрозам кіберзлочинності вважається за доцільне вжити на державному рівні наступні заходи:

1) законодавчі:

– завершити імплементацію в національне законодавство положень Європейської конвенції про кіберзлочинність, пов'язаних з документуванням злочинів у кіберпросторі, насамперед прийняти Закон України «Про перехоплення електронних комунікацій»;
– визначити поняття кібертероризму у ст. 1 Закону України «Про боротьбу з тероризмом», а також привести у відповідність з ним положення ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» [5, с. 86];
– внести зміни до Розділу XVI КК України в частині доповнення нормою про кримінальну відповідальність за кібернетичний терористичний акт, яка б дозволила розмежувати поняття кібертероризму та кіберзлочинності [5, с. 86], а також посилити кримінальну

відповідальності за незаконне втручання в роботу об'єктів критичної інформаційної інфраструктури;
- прийняти національну стратегію посилення кіберстійкості (на середньостроковий період), в якій передбачити розробку державних програм, фінансування досліджень, впровадження стандартів кібербезпеки тощо;

2) організаційні, насамперед спрямовані на удосконалення національної системи кібербезпеки, у т.ч.:
- забезпечити кіберстійкість та кібербезпеку національної інформаційної інфраструктури в умовах триваючої війни рф проти України та подальшої цифрової трансформації і розвитку системи кібербезпеки України;
- завершити формування національної системи управління кіберінцидентами, організованої на базі Єдиної системи управління інформаційною безпекою (SIEM) з використанням платформи MISP-UA, що дозволяє аналізувати стан інформаційної безпеки в режимі реального часу та оперативно виявляти, реагувати і попереджувати кіберзагрози на ОКІ та державним інформресурсам;
- упровадити ризик-орієнтований підхід до забезпечення кібербезпеки критичної інфраструктури держави, розробити методику ідентифікації та оцінки кіберзагроз та кіберризиків для ОКІ;
- запровадити обов'язковий аудит інформаційної безпеки на ОКІ, сформувати методики та основні алгоритми його проведення;
- упровадити універсальну систему індикаторів кіберзагроз, засновану на міжнародних стандартах з питань кібербезпеки та кіберзахисту;
- покращувати державно-приватну взаємодію у запобіганні кібератакам та кіберінцидентам на ОКІ, реагуванні на них, усуненні їх наслідків умовах кризових ситуацій, надзвичайного і воєнного стану;

3) режимні, контррозвідувальні й оперативно-розшукові, що спрямовані на зниження кіберзагроз:
- запровадити загальнодержавну систему виявлення й нейтралізації кібератак, протидії проявам кіберзлочинності й кібертероризму на ОКІ [5, с. 87];
- удосконалити наявну систему контррозвідувального забезпечення кібербезпеки держави, призначену для протидії кіберзагрозам;
- посилити моніторинг контенту мережі Інтернет (соціальні мережі, блоги, форуми та сервіси) та упроваджувати у практику новітні технологічні рішення, що надають доступ до інформації, що циркулює в мережі;
- забезпечувати постійне виявлення, запобігання і припинення актів кібертероризму та кібердиверсій, усунення їх причин і умов [5, с. 87];
- посилювати спроможності уповноважених органів у проведенні негласних перевірок стану готовності ОКІ до кібератак / кіберінцидентів;
- поліпшувати взаємодію уповноважених державних органів (СБУ, СЗРУ, НПУ, ДССЗЗІ) між собою та з компетентними органами іноземних держав, співпрацю з міжнародними організаціями, що протидіють кіберзлочинності в усіх її проявах (насамперед, з Інтерполом та Європолом).

Поширення кіберзагроз на усі сфери життєдіяльності держави і суспільства, пов'язані з функціонуванням критичної інформаційної інфраструктури в умовах повномасштабної військової агресії рф проти України, а також постійне вдосконалення інструментів їх реалізації зумовлюють необхідність зміни підходів у протидії кіберзлочинності під час війни.

Список використаних джерел:

1. Від початку року російські хакери активізували атаки проти України,– Юрій Мироненко. URL: https://cip.gov.ua/ua/news/vid-pochatku-roku-rosiiski-khakeri-aktivizuvali-ataki-proti-ukrayini-yurii-mironenko. (дата звернення: 18.06.2024)

2. Кількість зареєстрованих в Україні кіберінцидентів у 2023 році зросла на 62,5%,– Держспецзв'язку. 12.01.2024. URL: https://ms.detector.media/internet/post/33956/2024–01–12-kilkist-zareiestrovanykh-v-ukraini-kiberintsydentiv-u-2023-rotsi-zrosla-na-625-derzhspetszvyazku/.(дата звернення: 18.06.2024)

3. Поліковська Ю. Кіберфахівці СБУ щомісяця фіксують понад тисячу інформаційних атак на Україну. 30.11.2023. URL: https://ms.detector.media/kiberbezpeka/post/33614/2023–11–30-kiberfakhivtsi-sbu-shchomisyatsya-fiksuyut-ponad-tysyachu-informatsiynykh-atak-na-ukrainu/. (дата звернення: 18.06.2024)

4. Організаційно-правові основи забезпечення кібербезпеки: підручник / М.М. Присяжнюк, А.І. Марущак, Д.С. Мельник, В.В. Остроухов, М.В. Гуцалюк, О.П. Ткаченко; за заг. ред. М.М. Присяжнюка.– Київ: Вид-во «Ліра-К», 2023.– С. 82–125.

5. Мельник Д.С. Щодо потреби удосконалення законодавчого регулювання протидії кібертероризму в Україні. Проблеми правового забезпечнення національної безпеки в умовах війни та євроатлантичної інтеграції України: зб. матер. панельної дискусії в межах VII Харківського міжнародного юридичного форуму (м. Київ, 27.09.2023) / упоряд. Ю. Найдьон, В. Пилипчук, Т. Давидова. Київ: НА СБУ, 2023. С. 85–88.

ВІДПОВІДАЛЬНІСТЬ ЗА ВИКОРИСТАННЯ «БОТОФЕРМ», ЯК ІНСТРУМЕНТУ ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ НА ШКОДУ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Олександр МЕЛЬНІЧЕНКО
співробітник СБУ

Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України (далі – ДКІБ СБУ) відповідно до «Стратегії інформаційної безпеки України» затвердженої Указом Президента України № 685/2021 від 28.12.2021 року, за допомогою спеціальних форм та методів, організовано виявлення та протидію спеціальним інформаційним операціям, спрямованим на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації.

Інструментами ворожих спеціальних інформаційних операцій у кіберпросторі є: «ботмережі», блогери, інтернет-ресурси, спільноти та групи у соціальних мережах, керовані та фінансовані урядовими структурами рф.

Так, в 2024 році ДКІБ СБУ зафіксовано системне проведення спеціальних інформаційних операцій проти України, як елемента ведення агресивної війни рф, за наступними основними напрямками:

- дискредитація військово-політичного керівництва України;
- спроби зриву західної воєнної та фінансової підтримки України;
- схиляння України до мирних переговорів, на умовах агресора;
- дискредитація сил оборони України;
- дискредитація заходів загальної мобілізації в Україні;
- дестабілізація суспільно-політичної ситуації в Україні.

З початку повномасштабного вторгнення, ДКІБ СБУ встановлено численні факти активного використання «ботів» у соціально орієнтованих ресурсах мережі Інтернет під час проведення ворожих спеціальних інформаційних операцій на шкоду державній безпеці України.

«Ботами» є автоматизовані облікові записи в соціальних мережах, запрограмовані на певні дії, що імітують поведінку реальних інтернет-користувачів. Сукупність таких облікових записів,

запрограмованих на однакові дії та об'єднаних спільною метою, утворюють мережу ботів («ботмережу»), що характеризується наявністю великої кількості зв'язків у формі взаємної підписки на інші акаунти для відслідковування розміщення в них контенту та інших видів взаємодії.

З метою анонімізації своєї діяльності особи, причетні до керування «ботів», використовують різноманітні засоби, зокрема, віртуальні мобільні телефони, іноземні SIM-карти, віртуальні виділені сервери тощо.

Для створення та управління великою кількістю «ботів», використовуються спеціалізовані апаратно-програмні комплекси (т. зв. «ботоферми»). Вказані «ботоферми», як правило, включають в себе GSM-шлюзи, що використовуються також, для несанкціонованого втручання в роботу автоматизованих систем українських операторів мобільного зв'язку, блокування каналів зв'язку між обраними абонентами та базовими станціями провайдерів телекомунікацій шляхом автоматичної генерації великої кількості телефонних з'єднань (т.зв. «телефонний флуд»), а також використовуються для спам-розсилок українським користувачам, у тому числі для психологічного тиску на військовослужбовців сил оборони України.

Російськими спецслужбами, в інтересах ведення агресивної війни, нарощуються зусилля із створення «ботмереж», які містять недостовірні дані щодо користувачів на платформах соціальних мереж «Facebook», «Instagram» і «X» (колишній «Twitter»). Така діяльність з використання «бот-мереж» порушує політику конфіденційності та умови використання платформ вказаних транснаціональних ІТ-компаній.

Зокрема, відповідно до правил спільноти «Facebook» у соцмережі заборонено створювати профілі і сторінки, власники яких видають себе за інших людей або порушують умови використання «Facebook». У разі порушення користувачем правил платформи йому заборонено створювати інші облікові записи (акаунти) без дозволу «Facebook». Крім того, «Facebook» приділяє особливу увагу цілісності облікового запису і достовірності ідентифікаційних даних. Зокрема, грубим порушення правил спільноти є координація діяльності у рамках мережі облікових записів або інших об'єктів.

Правилами соціальної мережі «Instagram» не заборонено одному користувачу створювати кілька облікових записів (акаунтів), разом із тим політика платформи спрямована на протидію використанню підроблених облікових записів, при реєстрації яких використовуються ідентифікуючі дані інших осіб.

Відповідно до правил платформи «X» (колишній «Twitter»), користувачам заборонено використовувати недостовірні дані про особу, а саме фотографії профілю користувача, біографічні дані, інформацію щодо місцезнаходження профілю тощо.

Слід відзначити, що вказані ІТ-гіганти не приділяють достатньої уваги питанням протидії «ботмережам», оскільки це потребує додаткових фінансових витрат, не передбачено законодавством країн у юрисдикціях яких вони зареєстровані, і не становить будь-якого комерційного інтересу для власників цих компаній.

Разом з тим, Службою безпеки України з початку повномасштабного вторгнення рф, виявлено та припинено функціонування 86 ворожих «ботоферм» загальною потужністю близько 3 млн. акаунтів, діяльність яких координувалася рф та поширювалась на 12-мільйонну аудиторію, у різних регіонах України.

Відповідні процесуальні заходи відбувалися, за координації ДКІБ СБУ, в рамках кримінальних проваджень, зареєстрованих за статтями Кримінального кодексу України: 109 (посягання на конституційний лад України), 110 (посягання на територіальну цілісність України), 111 (державна зрада), 111–1 (колабораційна діяльність), 114–1 (перешкоджання законній діяльності Збройних Сил України та інших військових формувань в особливий період), 114–2 (несанкціоноване поширення інформації про переміщення ЗСУ), 161 (розпалювання міжнаціональної, міжрелігійної ворожнечі), 258–3 (сприяння терористичній організації), 436 (пропаганда війни), 436–1 (поширення комуністичної або нацистської символіки), 436–2 (виправдовування російської агресії проти України).

В той же час, безпосередньо діяльність зі створення та використання «ботоферм» і «ботмереж», на сьогоднішній день, не криміналізована в Україні, що дозволяє російським спецслужбам залучати громадян України до вказаної діяльності на шкоді інформаційній безпеці держави.

Таким чином, зважаючи на зростання негативних наслідків для держави у ході військової агресії рф проти України, які завдаються шляхом використання «ботоферм» та «ботмереж», що містять завідомо неправдиві відомості про користувача, для поширення недостовірної інформації (дезінформації), що загрожує національним інтересам України, або для впливу на прийняття чи не прийняття рішень органами влади чи публічними особами, потребує введення кримінальної відповідальності за вчинення таких дій.

Враховуючи викладене, пропонується розглянути питання щодо доповнення розділу I «Злочини проти основ національної безпеки України» Кримінального кодексу України статтею 114–3, якою встановити кримінальну відповідальність за створення та використання особою або групою осіб облікових записів (профілю користувача, веб-сторінки або електронної адреси), що містять завідомо неправдиві відомості про користувача, для поширення недостовірної інформації (дезінформації), що загрожує національним інтересам України, або для впливу на прийняття рішень чи вчинення або не вчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, за відсутності ознак державної зради.

З огляду на те, що вказане правопорушення створює загрозу інформаційній безпеці держави, яка є невід'ємною складовою національної безпеки України, вважається за доцільне віднести здійснення досудового розслідування кримінальних правопорушень до підслідності Служби безпеки України.

Список використаних джерел:

1. Указ Президента України № 685/2021 від 28.12.2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. (дата звернення: 19.06.2024)

2. Сайт СБУ. Забезпечення інформаційної безпеки. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky. (дата звернення: 19.06.2024)

3. Правила спільноти Facebook. URL: https://transparency.meta.com/uk-ua/policies/community-standard/ (дата звернення: 19.06.2024)

4. Правила спільноти Instagram. URL: https://help.instagram.com/477434105621119/?helpref=hc_fnav. (дата звернення: 19.06.2024)

5. Правила спільноти X. URL: https://help.twitter.com/ru/rules-and-policies/x-rules-and-best-practicesp. (дата звернення: 19.06.2024)

ПЕРСПЕКТИВИ ПРОЦЕСУАЛЬНОГО УНОРМУВАННЯ ПРОЦЕДУР БЛОКУВАННЯ ТА ПОВЕРНЕННЯ ЗЛОЧИННИХ ВІРТУАЛЬНИХ АКТИВІВ У ДОХІД ДЕРЖАВИ

Олексій МЕТЕЛЕВ
доктор філософії у галузі права,
завідувач кафедри Національного юридичного
університету імені Ярослава Мудрого

Проблема легалізації (відмивання) коштів має транскордонний характер і такі наслідки як: 1) фінансування організованої злочинності та тероризму; 2) заохочення корупції в державних органах і приватних установах; 3) зменшення державних доходів від оподаткування; 4) вплив на доброчесність бізнесу та фінансових установ, заохочення громадськості до втрати довіри до них; 5) підрив суспільної довіри до демократичних інституцій держави та її економіки.

По своїй суті, відмивання коштів полягає в тому, щоб гроші, які отримані від протиправної діяльності, провести крізь ланцюг операцій, маскуючи їхнє походження та інтегруючи їх до легальної фінансової системи.

Зазвичай відмивання коштів включає три етапи: 1) Розміщення: вкидання (введення) готівки до фінансової системи; 2) Приховування джерел («нашарування»): здійснення низки фінансових операцій для приховування незаконного походження коштів; 3) Інтегрування: гроші стають частиною фінансової системи й працюють в інтересах злочинців. Це класична схема відмивання коштів [1, с. 8].

Необхідно зазначити, що в результаті активного розвитку цифрових технологій в Україні сформувався особливий та якісно новий ринок обміну активами – ринок криптоактивів, які існують виключно у цифровій (нематеріальній) формі та істотним чином впливають на суспільно-економічні і правові відносини. При цьому, рівень популярності криптовалют серед українців постійно зростає. Україна, наразі, знаходиться у першій десятці країн за рівнем використання криптоактивів населенням. Криптовалюти, які є віртуальними активами, як явище існують вже довготривалий час і активно використовуються громадянами України, у тому числі для здійснення протиправної діяльності. Фактично ринок криптоактивів вже сформований та існує більше п'яти років, однак, він знаходиться повністю поза межами правового поля держави.

В існуючому «законодавчому вакуумі» обіг криптоактивів дає широкі можливості для відмивання «брудних» коштів і тісно пов'язаний з тіньовою економікою, фінансуванням тероризму і колабораціонізму, торгівлею зброєю та наркотичними речовинами тощо. При цьому цілком очевидно, що під час активної фази військової агресії з боку російської федерації щодо України, криптоактиви – це інструмент, який активно використовується не тільки криміногенними колами всередині країни задля задоволення злочинних інтересів, а й з метою підриву національної безпеки ззовні.

Одним із способів оплати товарів, робіт та технологій став стейблкоін Tether або USDT. Стейблкоїни (Assed referenced) за стандартами MiCA (нормативна база ЄС з регулювання криптовалют) – це криптоактиви, які мають забезпечувати стабільну ціну на базі вартості декількох фіатних валют, товарів, криптоактивів або комбінації таких активів [2, с. 12]. Можливість швидко перевести гроші в криптовалюту Tether, можливість міжнародних переказів без верифікації особи, а також можливість максимально анонімізувати походження коштів роблять даний вид розрахунків зручним для обходу санкцій, накладених на представників держави-агресора.

Як правило, органи досудового розслідування зазнають певних труднощів у процесі виявлення, документування та досудового розслідування кримінальних правопорушень, в яких під час вчинення злочинів у якості предмета посягання або платіжного засобу за протиправні дії чи послуги, а також призначеного для організації їх виконання, використовуються криптоактиви. У першу чергу, це пов'язано із умовною анонімністю володільців криптоактивів, а також, як вже зазначалось раніше, правовою невизначеністю статусу віртуальних активів та відсутністю в Україні державного або будь-якого іншого централізованого регулювання та контролю за їх обігом.

Майже у всіх кримінальних правопорушеннях, що відносяться до компетенції органів державної безпеки, криптоактиви, не зважаючи на їх високу волатильність, можуть використовуватись у якості умовного платіжного засобу для вчинення злочинів, а в тих з них, що відносяться до категорії корисливих, криптоактиви також можуть виступати об'єктом посягання.

Методика виявлення, документування та досудового розслідування кримінальних правопорушень, які відносяться до компетенції органів державної безпеки, та які пов'язані із використанням віртуальних активів, майже не відрізняється від аналогічних методик щодо таких злочинів із використанням класичних засобів платежу або використанням грошових коштів, іноземної валюти чи інших матеріальних цінностей, але має деякі відмінності.

Досить важливо, що виявлення механізму розрахунку криптовалютами за протиправні дії або послуги, заборонені або вилучені з обігу предмети, з метою встановлення місцезнаходжен-

ня криптовалюти, що виступила об'єктом протиправних посягань, можливо здійснити моніторинг криптовалютних транзакцій (операцій по переміщенню криптовалюти), оскільки вся інформація щодо транзакцій зберігається у системі блокчейн та доступна кожному користувачу Інтернет на відповідних веб-ресурсах, зокрема за допомогою сайтів blockchain.info, etherscan.io тощо. Також, зазначимо, що новітні інформаційні технології дозволяють швидко здійснювати вищезазначені транзакції без безпосереднього контакту ініціатора переказу із суб'єктом первинного фінансового моніторингу.

Теоретично кіберпростір не має обмежень (має транскордонний характер), тож, за наявності технічної можливості, існує вірогідність створення зловмисниками великої кількості віртуальних учасників (криптовалютних та електронних гаманців, віртуальних засобів платежу тощо) з метою переказу коштів, у тому числі цифрових.

Необхідно наголосити, що відповідно до статті 20 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, ратифікованої Законом України від 16 вересня 2014 року № 1678-VII (далі – Угода про асоціацію), Україна має забезпечити імплементацію відповідних міжнародних стандартів у сфері запобігання та боротьби з легалізацією (відмиванням) коштів та фінансуванням тероризму, зокрема стандартів Групи з розробки фінансових заходів боротьби з відмиванням коштів та фінансуванням тероризму (далі – FATF) [3].

В той же час, в Законі України від 06.12.2019 № 361-IX «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» існує визначення для віртуальних активів, яке наразі є застарілим та таким, що не дає можливості ефективно його використовувати в правозастосовній діяльності [4]. В експертному середовищі він відомий як AML-Закон (від англ. Anti-Money Laundering – протидія відмиванню коштів). Саме цей нормативно-правовий акт відповідає за імплементацію в законодавство України та фінансову сферу держави AML-політики, яка є комплексом заходів та процедур, що призначені для запобігання використання фінансової системи для відмивання грошей, тобто легалізації коштів (у тому числі криптоактивів), отриманих злочинним шляхом.

Оптимістично, що деякі законодавчі зміни щодо врегулювання віртуальних активів, все ж таки відбуваються. Так, відповідно до Закону України від 10.08.2023 № 3320-IX «Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав» віртуальні активи наразі визнаються в законодавстві цифровими речами, тобто є об'єктами цивільних прав [5]. Та це лише перші кроки. З урахування того, що навесні 2023 року Європейський парламент все ж таки прийняв єдиний регламент регулювання криптовалютного ринку в Європі, який охоплює регулювання багатьох складових криптоіндустрії у Євросоюзі – Регламент MiCA (від англ. Markets in Cryptoassets – ринки криптоактивів). Україна, взявши на себе зобов'язання, має зробити наступний крок на євроінтеграційному шляху та поступово імплементувати норми Регламенту MiCA у національне законодавство [6]. Саме тому, перед законодавцем постало нагальне питання щодо прийняття нового Закону України «Про віртуальні активи», який би по суті відповідав Регламенту MiCA.

Так, існуючий Закон України «Про віртуальні активи» від 17.02.2022 № 2074-IX, який мав би здійснювати регулювання правовідносин, що виникають у зв'язку з оборотом віртуальних активів (у тому числі криптоактивів) в Україні, визначати права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обороту віртуальних активів, так і не набрав чинності, оскільки перехідними положеннями даного законодавчого акту передбачено, що цей Закон набирає чинності з дня набрання чинності законом України про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами [7]. І хоча у Верховній Раді України ще у листопаді 2023 року зареєстровані два законопроекти «Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні», розроблені Національною комісією з цінних паперів та фондового ринку (№ 10225 від 07.11.2023)

та Міністерством цифрової трансформації України (№ 10225–1 від 17.11.2023), вони і досі знаходяться в процесі обговорення [8; 9].

Нажаль, у цих законопроектах відсутні пропозиції щодо внесення відповідних змін до Кримінального процесуального кодексу, які б унормовували процесуальні аспекти розслідування, документування, блокування, вилучення та повернення злочинних віртуальних активів в дохід держави. Водночас, відсутність таких процедур у кримінальному процесуальному законодавстві ставить під сумнів законність дій органів досудового розслідування під час кримінального провадження, які зараз поводяться з криптоактивами в одних випадках як з речовими доказами, а в інших як з документами.

Висновок. Отже, відсутність правового регулювання обігу криптоактивів та невизначеність повноважень уповноважених органів у сфері протидії їх злочинного використання змушує шукати дієві рішення не тільки для здійснення розвідки та пошуку злочинних криптоактивів, але й для здійснення належного управління замороженими (заарештованими) криптоактивами та їх подальшого повернення до держбюджету. Саме тому, ефективність проведення заходів щодо запобігання та протидії терористичній діяльності і розповсюдженню зброї масового знищення особливо залежить від своєчасного виявлення і блокування злочинних криптоактивів, що, відповідно, є одним із ключових напрямів реалізації порядку денного міжнародної та національної антитерористичної стратегії, а також важливим чинником у роботі всіх державних суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом у межах своєї компетенції. На думку автора, ефективне виконання уповноваженими органами заходів щодо протидії злочинного використання віртуальних активів для легалізації (відмивання) коштів, залежить від таких основних факторів:

1. Законодавче регулювання обігу криптоактивів та визначення повноважень правоохоронних органів у цій сфері, забезпечення безпеки якої є важливою складовою національної та державної безпеки.

2. Належна реалізація повноважень правоохоронних органів у сфері протидії злочинного використання криптоактивів, яка неможлива без ефективних методик та інструментів їх розслідування і виявлення, набуття чи використання яких пов'язані з фінансуванням тероризму, фінансуванням розповсюдження зброї масового знищення тощо.

3. Належна теоретична і практична підготовка співробітників правоохоронних органів у сфері обігу криптоактивів та набуття ними необхідних компетентностей у застосуванні методик та опанування основних інструментів розслідування злочинного використання криптоактивів.

В той же час необхідно зазначити, що саме недосконаліть (скоріше відсутність) законодавчого врегулювання обігу віртуальних активів, процедур їх блокування, вилучення та повернення у дохід держави створює суттєві перешкоди діяльності уповноважених органів по забезпеченню національної безпеки держави та уповільнює рух на шляху євроінтеграції України.

Список використаних джерел:

1. І. Ричардсон, І. де Лукас Мартін. Розслідування та судовий розгляд кримінальних проваджень щодо легалізації (відмивання) коштів: посібник для суддів. Стратсбург-Київ. 2021. 107 с.

2. Метелев О.П., Кононенко В.О., Мельниченко Д.С. Запобігання та протидія злочинам із використанням віртуальних активів підрозділами Служби безпеки України: практичний порадник. Київ, 2023. 78 с.

3. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Угоду ратифіковано із заявою Законом України від 16.09.2014 № 1678-VII. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 11.06.2024).

4. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового зни-

щення: Закон України від 06 грудня 2019 року № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361–20#Text (дата звернення: 11.06.2024).

5. Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав: Закон України від 10.08.2023 № 3320-IX. URL: https://zakon.rada.gov.ua/laws/show/3320-IX#Text (дата звернення: 07.06.2024).

6. Markets in Crypto-assets (MiCa): European Parliament legislative resolution of 20 April 2023 on the proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 (COM(2020)0593 – C9–0306/2020–2020/0265(COD)). URL: https://www.europarl.europa.eu/doceo/document/TA-9–2023–0117_EN.html (дата звернення: 11.06.2024).

7. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074–20#Text (дата звернення: 12.06.2024).

8. Проект Закону про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні від 07.11.2023 № 10225. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43132 (дата звернення: 01.06.2024).

9. Проект Закону про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні від 17.11.2023 № 10225–1. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43232 (дата звернення: 01.06.2024).

ТЕХНІЧНІ ЗАХОДИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Руслан МІРОШНИК
судовий експерт
Науково-дослідного центру судової експертизи
у сфері інформаційних технологій та інтелектуальної власності
Міністерства юстиції України

У сучасну цифрову епоху захист інформаційних систем від кіберзагроз має важливе значення для забезпечення безпеки даних, конфіденційності та цілісності систем. Впровадження надійних технічних заходів є критично важливим аспектом комплексної стратегії кібербезпеки. Захист інформаційних систем від широкого спектру кіберзагроз вимагає комплексного підходу, який включає численні технічні заходи. Дані заходи повинні працювати в тандемі, щоб забезпечити надійний захист різних компонентів інформаційної системи. Згідно із Законом України «Про захист інформації в автоматизованих системах» технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Ключовими технічними заходами для захисту інформаційних систем є:

Шифрування – це фундаментальний захід безпеки, який забезпечує конфіденційність і цілісність даних шляхом перетворення читабельних даних у нечитабельний формат, а також метод перетворення даних, щоб їх могли читати лише авторизовані особи. У процесі шифрування відкритий текст перетворюється в зашифрований за допомогою криптографічного ключа. Криптографічний ключ – це набір відомих математичних величин, погоджених як відправником, так і одержувачем. Дешифрування, або перетворення зашифрованих даних, виконується будь-якою особою, що має відповідний ключ. У більш безпечному шифруванні використовуються ключі високого рівня складності. Дані можуть бути зашифровані як під час зберігання, так і під час передачі. Основними видами шифрування є симетричне шифрування, асиметричне шифрування, хеш-функції, гібридне шифрування.

Симетричне шифрування використовує один і той же ключ для шифрування та дешифрування даних. Ключ повинен бути переданий між сторонами, що обмінюються інформацією. Популярними алгоритмами симетричного шифрування є: AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES). Сферами застосування симетричного шифрування являються: шифрування даних, що зберігаються (наприклад, шифрування баз даних), захист каналів зв'язку (наприклад, TLS/SSL), шифрування файлів.

Асиметричне шифрування використовує пару ключів, відкритий ключ для шифрування та закритий ключ для дешифрування. Відкритий ключ може бути поширений публічно, тоді як закритий ключ повинен залишатися секретним. Популярними алгоритмами асиметричного шифрування є: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography). Сферами застосування асиметричного шифрування являються: цифрові підписи, безпечний обмін ключами, шифрування невеликих обсягів даних.

Хеш-функції є важливим елементом у забезпеченні безпеки інформаційних систем. Вони використовуються для перевірки цілісності даних, створення цифрових підписів і зберігання паролів. Хеш-функція – це математичний алгоритм, який перетворює вхідні дані будь-якої довжини у вихідне значення, яке називається хешем або дайджестом. Популярними алгоритми хеш-функції є: SHA-256 (Secure Hash Algorithm 256-bit), SHA-3 (Secure Hash Algorithm 3), MD5 (Message Digest Algorithm 5), Bcrypt. Сферами застосування являються: перевірка цілісності даних, хешування паролів, цифрові підписи, криптографічні протоколи.

Гібридне шифрування поєднує симетричне та асиметричне шифрування, використовуючи їхні переваги. Зазвичай асиметричне шифрування використовується для безпечного обміну симетричним ключем, який потім використовується для шифрування даних. Сферами застосування являються: захищені комунікаційні протоколи, такі як HTTPS і PGP (Pretty Good Privacy).

Аутентифікація, авторизація та ідентифікація є ключовими компонентами забезпечення безпеки інформаційних систем. Вони працюють разом, щоб гарантувати, що лише уповноважені користувачі мають доступ до певних ресурсів і можуть виконувати визначені дії.

Ідентифікація – це процедура розпізнавання суб'єкта. Цього можна досягти за допомогою ідентифікатора користувача (наприклад, логін), ідентифікатора процесу тощо. Дуже важливо, щоб заявлені облікові дані були унікальними, щоб можна було розрізняти різні суб'єкти в системі. Тобто у системі не може бути зареєстровано два однакових ідентифікатора, два однакових номери телефону, дві однакові електронні пошти і так далі.

Після того, як суб'єкт ідентифікує себе, його потрібно аутентифікувати. Аутентифікація (Authentication) – це процес перевірки особи користувача, пристрою або сутності, яка намагається отримати доступ до системи або ресурсу. Цей доказ ідентичності досягається шляхом надання облікових даних механізму контролю доступу. Також перевіряється дійсність наданих облікових даних перед тим, як затвердити запит на аутентифікацію. Іншими словами, аутентифікація визначає, що суб'єкт як володіє, так і контролює надані облікові дані (аутентифікатори). Деякими прикладами облікових даних, які можна використовувати для підтвердження особи, є паролі, PIN-коди, цифрові підписи, біометричні дані тощо.

Авторизація – це процес визначення рівня доступу користувача до ресурсів або дій після того, як його особа була підтверджена через аутентифікацію. Основна мета авторизації гарантувати, що користувачі мають лише ті права і привілеї, які їм необхідні для виконання своїх завдань, та запобігти несанкціонованому доступу до критичних систем і даних.

Забезпечення доступу до інформаційних систем лише авторизованим користувачам має вирішальне значення для безпеки.

Мережева безпека – є критичним аспектом захисту інформаційних систем від різноманітних загроз та атак. Вона включає в себе методи, стратегії та технології, які забезпечують захист від несанкціонованого доступу, витоків даних, зловмисних дій та інших кіберзагроз. Захист мережевої інфраструктури запобігає несанкціонованому доступу та виявляє зловмисні дії. Основними методами та технологіями мережевої безпеки є: брандмауери для контролю вхідного та вихідного мережевого трафіку на основі заздалегідь визначених правил безпеки.

Брандмауери діють як бар'єр між довіреними та недовіреними мережами, блокуючи потенційно шкідливий трафік; системи виявлення та запобігання вторгнень (IDS/IPS) для моніторингу мережевого трафіку на предмет підозрілої активності та вжиття заходів для запобігання потенційним загрозам. IDS/IPS можуть ідентифікувати та блокувати шкідливий трафік, захищаючи мережу від атак.

Безпека кінцевих точок має важливе значення для захисту всієї інформаційної системи. Під цим терміном маються на увазі кінцеві пристрої в мережі: робочі станції, ноутбуки, планшети, смартфони, сервери. Кожне робоче місце співробітника організації та будь-яке периферійне устаткування, підключене до мережі – це кінцева точка, яка може стати об'єктом атаки. Відсутність належного захисту цього сегмента корпоративної мережевої інфраструктури може призвести до катастрофічних наслідків. Оскільки на даний час більшість спроб проникнення здійснюється через кінцеві точки, централізованого захисту мережі, що використовувався раніше, вже недостатньо. Однією з найбільш передових технологій запобігання атак є рішення на базі Endpoint Detection and Response (EDR). EDR – це комплексна система, що являє собою набір технологій, призначених для моніторингу, зображення і зберігання даних, які відстежують всі дії, що відбуваються в кінцевих точках. Ці дані збираються в централізованому сховищі де аналізуються. Захист проводиться в реальному часі, і якщо в процесі аналізу EDR виявить в якійсь із точок ознаки злому, автоматично починають використовуватися можливості швидкого реагування, а після усунення загрози відбувається відновлення до безпечних параметрів функціонування. Однією з найбільш небезпечних загроз, яку можуть зазнати віддалені пристрої, є fileless атаки. Їх особливість полягає в тому, що кіберзлочинцям не потрібно розміщувати файли на жорсткому диску атакованого пристрою. Найчастіше для здійснення злому використовуються вже встановлені на планшеті або смартфоні додатки, що знаходяться в схваленому списку. Для виявлення в кінцевих точках таких загроз добре підходять системи, засновані на технології EDR. Вони здійснюють постійний контроль додатків, запущених на мобільному пристрої, забезпечуючи його захист.

Оновлення програмного забезпечення та системи є важливим аспектом забезпечення кібербезпеки та функціональної стабільності інформаційних систем. Вони дозволяють усунути вразливості, покращити продуктивність, додати нові функції та забезпечити сумісність з іншими системами. Регулярні оновлення та управління виправленнями мають вирішальне значення для захисту від відомих вразливостей, а саме: оновлення безпеки, які виправляють уразливості, якими можуть скористатися кіберзлочинці, щоб отримати несанкціонований доступ, викрасти дані або порушити роботу; оновлення функцій, впроваджує нові функціональні можливості та можливості в програмне забезпечення або системи, покращуючи взаємодію з користувачем і продуктивність; оновлення продуктивності, оптимізує програмне забезпечення або системний код для підвищення швидкості, ефективності та загальної продуктивності; оновлення сумісності, гарантує, що програмне забезпечення або система залишаються сумісними з новим обладнанням, операційними системами чи іншими програмами; виправлення помилок, усуває відомі проблеми, які можуть спричинити збій у роботі програмного забезпечення або видавати помилки.

Резервне копіювання та відновлення забезпечують захист від втрати даних через апаратні збої, помилки користувачів, кібератаки та інші непередбачені події. Основними видами резервного копіювання є: повне резервне копіювання (Full Backup) – створення копії всіх даних, що забезпечує повне відновлення у разі втрати даних; інкрементне резервне копіювання (Incremental Backup) – копіювання тільки тих даних, що були змінені з моменту останнього резервного копіювання (повного або інкрементного); диференційне резервне копіювання (Differential Backup) – копіювання всіх змінених даних з моменту останнього повного резервного копіювання; безперервне резервне копіювання (Continuous Data Protection, CDP) – постійне копіювання даних у реальному часі, що забезпечує найактуальніші копії даних для відновлення.

Моніторинг та ведення журналів є важливими складовими частинами управління безпекою інформаційних систем. Ці процеси дозволяють вчасно виявляти та реагувати на загрози,

здійснювати моніторинг стану систем та забезпечувати дотримання нормативних вимог. Безперервний моніторинг і реєстрація допомагають виявляти та реагувати на інциденти безпеки в режимі реального часу. Основними аспектами моніторингу та ведення журналів є: управління інформацією та подіями безпеки (SIEM), рішення для збору, аналізу та кореляції даних про події безпеки з різних джерел. SIEM забезпечує моніторинг у режимі реального часу та сповіщення про потенційні інциденти безпеки; ведення повних журналів системної активності, включаючи журнали доступу, журнали помилок і журнали транзакцій. Регулярний перегляд журналів для виявлення незвичних або підозрілих дій.

Сегментація мережі є важливим методом підвищення безпеки, продуктивності та управління мережевою інфраструктурою. Цей підхід полягає у розділенні мережі на менші, ізольовані сегменти, кожен з яких має свої політики доступу та безпеки. Ізоляція критично важливих систем і даних обмежує поширення атак всередині мережі. Сегментація мережі забезпечує розмежування між сегментами, зменшуючи вплив скомпрометованого сегмента.

Також впровадження віртуальних локальних мереж (VLAN) для створення ізольованих мережевих сегментів у фізичній мережі допомагає контролювати потік трафіку і підвищують безпеку, обмежуючи доступ до чутливих ділянок.

Тестування безпеки є важливим елементом забезпечення кібербезпеки організації та дозволяє виявити вразливості, оцінити рівень захищеності інформаційних систем та впровадити необхідні заходи для усунення ризиків. Тестування на проникнення проводиться з метою, щоб змоделювати реальні атаки та виявити слабкі місця в системі. Результати тестування використовуються для посилення захисту та усунення вразливостей. Автоматизовані та ручні оцінки вразливостей виконуються щоб виявити та усунути недоліки в системі безпеки.

Навчання та обізнаність користувачів кібербезпеці є критично важливими для захисту інформаційних систем організацій. Людський фактор залишається однією з найслабших ланок в ланцюгу кібербезпеки, тому підготовка та навчання персоналу можуть значно знизити ризики. Проведення регулярних тренінгів для співробітників на такі теми, як фішинг, безпека паролів та безпечний перегляд веб-сторінок. Впровадження постійних програми з підвищення обізнаності про безпеку.

Впровадження цих технічних заходів має важливе значення для створення надійного захисту від кіберзагроз та захисту інформаційних систем. Поєднуючи шифрування, надійну аутентифікацію, мережеву безпеку, захист кінцевих точок, регулярні оновлення та ретельний моніторинг, можливо значно знизити ризик кібератак. Крім того, включення фізичної безпеки, DLP, IAM, безпеки додатків, хмарної безпеки, реагування на інциденти, SOAR, MDM та постійне навчання з питань кібербезпеки ще більше посилить загальний стан безпеки та стійкість до потенційних загроз.

Список використаних джерел:

1. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 17.06.2024).

2. Defensive Security Handbook, O' Reilly Media, Inc, April 2017, URL: https://learning.oreilly.com/library/view/defensive-security-handbook (дата звернення: 17.06.2024).

3. Nathan House, The Complete Cyber Security Course, London, 2016, 273 с.

4. QATestLab, URL: https://training.qatestlab.com/blog/technical-articles/ (дата звернення: 17.06.2024).

5. iIT Distribution, URL: https://iitd.com.ua/zashchita-konechnyh-tochek/ (дата звернення: 18.06.2024).

ЗАХИСТ КУЛЬТУРНОЇ СПАДЩИНИ УКРАЇНИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ: КРИМІНАЛІСТИЧНІ ТЕХНОЛОГІЇ ТА ІННОВАЦІЇ

Владислав НЕГРЕБЕЦЬКИЙ
кандидат юридичних наук, доцент,
науковий співробітник НДІ вивчення проблем злочинності
імені академіка В.В. Сташиса НАПрН України

У зв'язку війною на Україні особлива роль відводиться роботі правоохоронних органів щодо забезпечення інформаційної безпеки у всіх життєво важливих галузях функціонування держави. В Україні атакують і бомбардують не лише військові частини, але й варварське руйнують критичну інфраструктуру, зокрема житлові квартали, гинуть мирні жителі та навіть діти. Порушуються основні принципи міжнародного співробітництва та норми міжнародного права. Український народ захищає не лише свою країну, націю, а й незалежність інших європейських держав, а також фундаментальні принципи міжнародного права: демократію, права і свободи людини, верховенство права та нашу спільну безпеку на даний момент і назавжди, майбутнє всього людства. Особливо важка ситуація в регіонах, де ведуться активні бойові дії. На сході України нещадних бомбардувань зазнає Харків, де зосереджено чимало визначних пам'яток української культури, принципово важливих для її історії. Серед постраждалих пам'яток у середмісті Харкова – будівля Харківського художнього музею, зведена ще 1912 р. як особняк за проектом видатного українського зодчого О. Бекетова. Унаслідок бомбардувань постраждала й Харківська державна наукова бібліотека ім. В.Г. Короленка, побудована в 1899–1901 рр. так само за проектом О. Бекетова.. Порушуються основні принципи міжнародного співробітництва та норми міжнародного права.

Згідно даних Генерального прокурора України в Україні станом на 21.06.2024 р. розслідувалось понад 134 300 справ про воєнні злочини держави – агресора. Зафіксовані чисельні випадки руйнувань житлової інфраструктури, вбивств мирних жителів, мародерства та насильства. Наразі на сайті Міністерства культури та інформаційної політики України зафіксовано 513 пошкоджених та зруйнованих об'єктів культурної спадщини й культурних установ України.

Національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Національні інтереси України – це життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян.

Як відзначають науковці Національної бібліотеки України імені В.І. Вернадського, широкомасштабне вторгнення на територію України 24 лютого 2022 р. спровокувало чи не найбільшу за останні 80 років світову кризу – гуманітарну, кризу міжнародного права і міжнародних інституцій, а також поставило під загрозу величезний пласт європейської культурної спадщини. Під час бойових дій багато об'єктів культурної спадщини України, зокрема церкви, музеї, архітектурні та скульптурні споруди, бібліотеки та інші історичні і культурні пам'ятки перебувають під загрозою руйнування або пошкодження, а деякі вже зазнали їх. Зрозумілим видається занепокоєння ЮНЕСКО з цього приводу – на території України знаходиться сім об'єктів Світової спадщини, зокрема розташованих у Львові та Києві; міста Одеса та Харків входять до мережі творчих міст, а деякі національні архіви України включено до Реєстру ЮНЕСКО «Пам'ять світу». Сьогодні актуальним питанням залишається широка імплементація в національне, зокрема кримінальне законодавство України норм міжнародного гуманітарного права та між народного права охорони культурних цінностей.

Центр протидії дезінформації (далі – Центр) є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106. Центр підпорядкований Раді національної безпеки і оборони України. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Зокрема, до завдань Центру належать:

проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі;

виявлення та протидія дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Так, із 2014 року ворог активно намагається просувати фейки про історію півдня України, що направлені на історичні маніпуляції в інформаційному просторі не тільки України, але і всього світу. Центр протидії дезінформації проводить дослідження інформаційного простору з метою виявлення ворожих кампаній зокрема, стосовно культурної спадщини України. З цією метою послідовно проводилась компанія з розміщення на інформаційних ресурсах фейків.

Фейком у перекладі з англійської «fake» означає – «фальшивка», «підробка», «обман». Таким чином, фейк – це завідомо неправдива інформація. Дезінформація – відомості, що розраховані на введення особи в оману.

Нещодавно Центр протидії дезінформації оприлюднив результати дослідження, в якому пояснив як саме проводиться дезінформаційна кампанія з використанням особливостей «української психології».

Чітко виділяються критерії, яким має відповідати таке повідомлення:

– Фейк повинен бути банальним. Щоб впливати на широкі шари суспільства, не потрібно придумувати нічого надприродного. Краще додати навіть трохи абсурду;
– Фейк повинен мати в собі потужний меседж і залишати простір для власних фантазій;
– Фейк має враховувати місцеві особливості. Достовірності йому придає прив'язка до місцевості;
– Багаторазове повторення.

При цьому Центр протидії дезінформації підкреслює всю серйозність і масштабу інформаційної війни.

Нещодавно Центр протидії дезінформації презентував новий інноваційний інструмент для поротьби з фейками – фактчек-бот «Перевірка». Перевірка – бот від журналістів @gwaramedia для виявлення сумнівної інформації та суперечливих фактів. Це бот-рятівник від фейкових новин, неперевіреної інформації, відвертої брехні, пропаганди. Він допоможе розрізнити фейкові новини у соцмережах, у політиці, визначити фейкові новини російських ЗМІ, спрямовані на боротьбу з Україною.

За допомогою цього інструменту можна надіслати ботові новини, статті, фото, посилання, повідомлення. Надішліть інформацію, яку хочете перевірити на справжність. Ваше посилання відразу потрапляє команді, яка вміє швидко перевіряти великі масиви інформації із застосуванням штучного інтелекту. За результатами проведеної перевірки протягом декількох хвилин буде надано відповідь, чи правдива надіслана інформація. Відповідь надійде протягом доби.

Для протидії дезінформації необхідно виробити у суспільства інформаційний імунітет. Інформаційний імунітет – це здатність ідентифікувати маніпуляцію, фейк, оцінити рівень їх небезпеки і як їм можна запобігти.

Це завдання можна досягнути лише за допомогою підвищення медіаграмотності та дотримання правил інформаційної гігієни, зокрема:

– отримувати інформацію лише з офіційних джерел;

– не варто реагувати на занадто емоційні повідомлення;
– не поширювати неперевірену інформацію.

Питання розвитку інформаційного імунітету у Українського суспільства є вельми актуальним і пріоритетним на шляху до Перемоги. Але, не менш важливим стратегічним напрямком у боротьбі з дезінформацією є розробка всебічного та ґрунтовного підходу до протидії з цим явищем в Україні з урахуванням стандартів Ради Європи та досвіду країн ЄС. Нещодавно Рада Європи ухвалила низку стандартів, які в комплексі сприятимуть протидії інформаційному безладу, зокрема:

Резолюція парламентської асамблеї Ради Європи «Демократія зламана? Як відповісти?» (Democracy hacked? How to respond?) № 2326, в якій ПАРЄ висловила стурбованість у зв'язку з поширенням дезінформаційних кампаній, спрямованих на формування суспільної думки, тенденцій маніпуляцій та іноземного втручання у виборчі процеси;

Рекомендація CM/Rec(2018)2 про роль та відповідальність Інтернет посередників;

Рекомендація CM/Rec(2020)1 щодо впливу алгоритмічних процесів на права людини та інші документи.

Вважаємо, що для ефективного подолання дезінформації необхідно реалізувати в Україні ці стандарти Рада Європи. В той же час, необхідно підвищити роль сучасних інформаційних систем на основі штучного інтелекту, орієнтованих на оперативне реагування і протидію дезінформаційним операціям з боку країни-агресора.

Список використаних джерел:

1. Звернення. (04.03.2022) URL: https://crimcongress.com/news/звернення/. (дата звернення 21.06.2024)

2. У Харкові 24 історичні будівлі пошкоджені внаслідок ударів РФ 16 січня (18 січня 2024). URL: https://suspilne.media/kharkiv/664194-u-harkovi-vnaslidok-udariv-rf-16-sicna-poskodzeni-24-istoricni-budivli/. (дата звернення 21.06.2024)

3. Офіс Генерального прокурора. URL: https://www.gp.gov.ua/ (дата звернення 21.06.2024)

4. 1987 об'єктів культурної інфраструктури зазнали пошкоджень чи руйнувань через російську агресію (02.05.2024). URL: https://mcip.gov.ua/news/1987-obyektiv-kulturnoyi-infrastruktury-zaznaly-poshkodzhen-chy-rujnuvan-cherez-rosijsku-agresiyu/. (дата звернення 21.06.2024)

5. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469–19#Text. (дата звернення 20.06.2024)

6. Кара-Васильєва Т.В. Культурна спадщина України: дослідження, її стан у період новітніх викликів сучасності. Вісник Національної академії наук України.– 2022.– № 7.– С. 42–46. URL: http://nbuv.gov.ua/UJRN/vnanu_2022_7_13. (дата звернення 21.06.2024)

7. Центр протидії дезінформації. URL: https://cpd.gov.ua/. (дата звернення 20.06.2024)

8. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. № 106/2021. URL: https://www.president.gov.ua/documents/1062021–37421. (дата звернення 20.06.2024)

9. Російські фейки про історію півдня України: на них будується пропаганда. (23.01.2022). URL: https://www.radiosvoboda.org/a/novyny-pryazovya-rosiyski-mifi-pivden-ukrayiny/31667316.html. (дата звернення 20.06.2024)

10. Велика українська юридична енциклопедія: У 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол. В.Ю. Шепітько та ін. Харків: Право, 2018. 952 с.

11. Російська пропаганда підготувала «посібники» для створення фейків! URL: https://www.facebook.com/protydiyadezinformatsiyi.cpd/posts/133802149168859. (дата звернення 20.06.2024)

12. Бот ПЕРЕВІРКА URL: https://t.me/perevir_bot. (дата звернення 21.06.2024)

13. Протидія дезінформації: європейські підходи та стандарти. URL: https://www.coe.int/uk/web/kyiv/-/responding-to-disinformation-european-practices-and-standards (дата звернення 20.06.2024)

ДО ПИТАННЯ ВДОСКОНАЛЕННЯ КОНЦЕПЦІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Наталія НЕТЕСА
кандидат юридичних наук, старший дослідник,
вчений секретар Науково-дослідного
інституту вивчення проблем злочинності
імені академіка В.В. Сташиса НАПрН України

Забезпечення захищеності інформаційного простору України є одним із пріоритетних завдань державної політики воєнного часу, адже інформаційний простір не лише відкриває широкі можливості для формування та укріплення національно-державницької ідеології, а й є зручною віртуальною ареною для здійснення різноманітних маніпулювань суспільною свідомістю, що загрожує суспільно-політичною дестабілізацією в державі зі всіма випливаючими з цього наслідками, передусім зниження обороноздатності країни, послаблення підтримки України з боку міжнародної та світової спільноти і, врешті-решт, консолідації українського суспільства у справі протистояння ворогу. Сьогодні, на третьому році повномасштабного вторгнення рф в Україну, особливо гостро відчувається потреба в органічному поєднанні психологічного, технологічного та інформаційного інструментарію заради того, щоб не допустити втому населення від війни, посилення конфронтації політиків та військових, загострення соціальних розколів по найважливіших лініях: «воював – не воював», «внутрішньо переміщена особа – місцевий мешканець», «залишився в Україні – виїхав за кордон», «військовий – цивільний», «фронтовий – тиловий», «офіцер – рядовий» та ін. [1, с. 113] Все це живить ґрунт для розхитування суспільно-політичної ситуації в Україні, збільшення масштабів колабораційної діяльності, пособництва агресору тощо. І тут далеко не останню роль набуває здійснення свідомої, соціально відповідальної інформаційної діяльності насамперед публічними особами, які мають доступ до так званої чутливої в умовах війни інформації, виток якої здатен заподіяти шкоду національній безпеці та обороні України. Крім того, прагнення до нарощування власних рейтингів політичними та громадськими діячами, представниками медіаспільноти та іншими лідерами громадської думки нерідко має своїм наслідком поширення інформації з деструктивним контентом, в тому числі з метою маніпулювання громадською думкою.

Здавалося б, на сьогодні в Україні наявна достатньо потужна правова платформа у сфері забезпечення її інформаційної безпеки. Так, окрім базових законів у цій сфері, в нашій державі прийнято цілу низку документів стратегічного характеру, серед яких Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020, Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021, Стратегія воєнної безпеки України, затверджена Указом Президента України від 21.03.2021 р. № 121/2021, Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.2022 р. № 56/2022, а також відповідні Плани заходів, спрямовані на реалізацію указаних Стратегій. Проте, як бачимо, перелічені Стратегії розроблені до початку повномасштабного вторгнення рф в Україну, а їх системний аналіз показав, що з того часу жодного оновлення ці документи не зазнавали. Більше того, й Плани заходів з реалізації цих Стратегій, окремі з яких були прийняті вже після подій 24 лютого 2022 р., свідчать про формальність підходу до виконання поставлених стратегічних завдань у сфері забезпечення інформаційної безпеки, доказом чого є зміст індикаторів їх виконання, на кшталт, «підготовлено звіти за результатами моніторингу», «проведено заходи», «внесено пропозиції», «поширено інформаційні матеріали», «проведено аналіз інформаційного простору» тощо [2, 3]. Цілком очевидно, що такі індикатори аж ніяк не відповідають вимогам умов воєнного стану. Прикладом «моральної застарілості» ключових у цій сфері нормативних документів є й те, що

досі в них фігурують як тимчасово окуповані лише АРК та окремі райони Донецької та Луганської областей [3, 4], а у Плані заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, затв. розпорядженням Кабінету Міністрів України від 30 березня 2023 р. № 272-р, станом на грудень 2023 р. прозвітовано про виконання стратегічного завдання «Забезпечення інформування світової спільноти про події в Україні та донесення офіційної позиції України до представників іноземних держав і медіа» реалізацією такого заходу, як «оновлення глосарію назв, термінів та словосполучень, які рекомендовано для використання органами державної влади та органами місцевого самоврядування, дипломатичними представництвами України, медіа, організаціями громадського сектору у зв'язку з тимчасовою окупацією рф Автономної Республіки Крим, м. Севастополя та окремих районів Донецької і Луганської областей» [3]. І це після 1 року і 10 місяців повномасштабної збройної агресії, коли під окупацією опинилися також частина південних та східних територій, зокрема Херсонської та Харківської областей. Крім того, викликає подив й те, яке місце у реалізації заходів відводиться Службі безпеці України, адже у більшості пунктів зазначеного Плану заходів цей орган вказаний серед відповідальних виконавців як такий, що бере участь у реалізації заходів «за згодою», а в окремих випадках або не зазначений взагалі, або зазначений на останніх позиціях, як наприклад, у реалізації заходів щодо протидії дезінформації та спеціальним інформаційним операціям, спрямованим на підрив конституційного ладу, суверенітету і територіальної цілісності України, а також дискредитацію євроатлантичного та європейського стратегічного курсу держави [3].

Вочевидь, що такий стан справ у забезпеченні інформаційної безпеки в державі в умовах воєнного часу не може бути визнаний задовільним і зумовлює необхідність зміни підходів, що має супроводжуватися розробкою нової Концепції забезпечення інформаційної безпеки саме в умовах воєнного стану з розширенням повноважень СБУ як державного органу спеціального призначення з правоохоронними функціями, відповідального за забезпечення національної безпеки України, у тому числі в інформаційній сфері. Така Концепція має передбачати, поряд із вже традиційними, низку додаткових заходів зі зміцнення інформаційної безпеки з урахуванням збільшення обсягу територій тимчасової окупації, продовження режиму воєнного стану, зміни тактики й стратегії ведення бойових дій та здійснення спеціальних інформаційних операцій супротивником, а також з огляду на вже чітко окреслені внутрішньодержавні чинники (мовні, релігійні, ідеологічні, соціально-демографічні, воєнно-політичні), що розхитують суспільно-політичну ситуацію в Україні, а також з усвідомленням потреби в активізації інформаційної діяльності у зовнішньому інформаційному просторі. Зокрема, наразі гостро відчувається потреба в активізації протидії спеціальним інформаційним операціям рф проти України в інформаційному полі держави-агресора, що може бути забезпечено за рахунок розширення присутності українських спецслужб в інформаційному просторі супротивника та посилення інформаційного впливу на його аудиторію (в тому числі окремі цільові групи: підліткові, релігійні, військові та ін.), формування та розширення агентурної мережі серед громадян країни-агресора та жителів тимчасово окупованих територій з метою здійснення розвідувальної та диверсійно-підривної діяльності в інформаційному просторі супротивника задля поширення панічних настроїв, загострення суспільно-політичної обстановки, поглиблення соціальних розколів у суспільстві супротивника. Окремим напрямом вдосконалення механізму забезпечення інформаційної безпеки держави має стати упровадження дієвих механізмів взаємодії суб'єктів забезпечення інформаційної безпеки, в тому числі СБУ, з інститутами громадянського суспільства, насамперед з аналітичними центрами, грантовими організаціями, call-центрами, які збиратимуть суспільно важливу інформацію щодо деструктивних тенденцій у політичній, воєнній, соціальній, економічній, релігійній, ідеологічній та інших сферах життєдіяльності суспільства та спрямовуватимуть її до спецслужб та створеного єдиного інформаційного центру для подальшої обробки й ретельного моніторингу на предмет наявності потенційних ризиків для інформаційної безпеки та вжиття заходів щодо адекватного реагування на такі загрози в інформаційній сфері. Так само соціально виправданим в умовах воєнного стану є більш активне залучення СБУ до формування інформаційної повістки з питань забезпечення інформаційної безпеки в контексті військової

складової, діяльності спецслужб та загальносуспільних питань, висвітлення яких в умовах воєнного стану в інформаційному просторі має перебувати в зоні координації спецслужб, а також посилення напряму кураторства з боку СБУ за формуванням проукраїнських наративів і меседжів та забезпечення їх трансляції через відповідні офіційні та інші канали. Безумовно, свого посилення потребує і взаємодія СБУ з лідерами громадської думки (зокрема блогерами) у напрямку поширення в інформаційному просторі контенту, спрямованого на консолідацію українського суспільства, а також контенту, що провокує посилення соціальних розколів у державі-агресорі. Таке зміщення акцентів саме у площину інформаційного простору зумовлює необхідність й в одночасному нормативному обмеженні кола осіб, які уповноважені офіційно представляти органи державної влади й місцевого самоврядування в інформаційному просторі, в тому числі у статусі так званих «воєнних експертів», а також у посиленні відповідальності публічних осіб за публічне поширення чутливої в умовах воєнного стану інформації як всередині країни, так і ззовні, що може бути реалізовано через доповнення низки норм Кримінального кодексу України (що передбачають відповідальність за поширення відповідної інформації, публічні заклики, пропаганду, розголошення відомостей та ін.) відповідною кваліфікуючою ознакою.

Список використаних джерел:

1. Нетеса Н.В. Основні внутрішьодержавні чинники, що зумовлюють загрози інформаційній безпеці України в умовах воєнного стану. Кримінальне право України періоду глобальних викликів: від воєнного стану до повоєнного відродження: матеріали дискус. кримін.– прав. панелі VII Харків. міжнар. юрид. форуму (м. Харків, 29 верес. 2023 р.): електрон. наук. вид. / редкол.: В.С. Батиргареєва (голова), Ю.А. Пономаренко, Д.П. Євтєєва та ін.; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; Нац. юрид. ун-т ім. Ярослава Мудрого.– Харків: Право, 2023. С. 111–114.

2. Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: розпорядження Кабінету Міністрів України від 18 квітня 2023 р. № 328-р. URL: https://zakon.rada.gov.ua/laws/show/328–2023-%D1%80#Text. (дата звернення 17.06.2024)

3. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272–2023-%D1%80#Text. (дата звернення 17.06.2024)

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021–41069. (дата звернення 17.06.2024)

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ОРГАНАМИ ТА ПІДРОЗДІЛАМИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Денис ОЛЄЙНІКОВ
кандидат юридичних наук,
професор Національного юридичного
університету імені Ярослава Мудрого

Статтею 17 Конституції України передбачено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1]. Цілком зрозуміло, що реалізація означеної функції має отримати відповідний механізм, який би дозволяв визначеним законом суб'єктам повною мірою виконувати поставлені на них завдання з захисту та забезпечення

інтересів держави у сфері інформаційної безпеки. Існування ж та функціонування такого механізму має бути врегульовано достатньою нормативно-правовою базою, яка б забезпечила безперебійну роботу в означеному вище напрямі.

Інформаційна безпека України у Стратегії інформаційної безпеки України, затвердженій Указом Президента України від 28 грудня 2021 року № 685/202, визначається як складова національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Автори монографічного дослідження правових засад інформаційної безпеки України перелічили критичні структури, які, згідно Концепції міжнародної інформаційної безпеки, у першу чергу зазнають впливу в умовах інформаційного протиборства. Найбільш вразливими, на думку вказаних фахівців, вважаються політична, суспільна, економічна, військова, науково-технологічна, духовна сфери життєдіяльності суспільства, а саме:

- у політичній сфері інформаційна безпека стосується всіх елементів політичної структури держави та суспільства: структур підготовки та прийняття політичних рішень, структур управління місцевої та регіональної влади, структур виборчих систем, інформаційно-телекомунікаційних урядових систем спеціального призначення;
- для економічної сфери критичними вважаються системи загальноекономічного аналізу та прогнозування економічного розвитку, структури прийняття рішень та координації управлінських дій в економічній сфері, зокрема, в умовах надзвичайного стану, інфраструктури банківських мереж і систем, системи управління в критично важливих для функціонування держави структурах (енергетика, транспортні комунікації, телекомунікаційні та інформаційні мережі);
- у військовій сфері вразливими в умовах інформаційного протиборства вважаються інформаційні ресурси збройних сил, військово-промисловий комплекс, системи управління військами, системи контролю і постійного спостереження, канали надходження інформації стратегічного, оперативного, тактичного, розвідувального характеру;
- глобальними загрозами в науково-технологічній сфері є феномен транскордонного переміщення інтелектуальних ресурсів, тобто вивезення інформації унікального науково-технологічного характеру на біологічних носіях до міжнародних систем спостереження, аналізу і прогнозування тенденцій науковотехнологічного розвитку в різних країнах з метою доступу до об'єктів критичної інфраструктури, до конфіденційних баз і банків даних; критичними для безпеки у сфері науки і технологій є структури накопичення науково-технічної інформації, інструкції та структури фундаментальних і прикладних досліджень, об'єкти інтелектуальної власності, ноу-хау;
- суспільна сфера є найбільш вразливою для інформаційних впливів, оскільки включає системи формування громадської думки, структури засобів масової комунікації, інформаційно-організаційні структури політичних партій, громадських рухів, національно-культурних та релігійних інституцій, структури забезпечення основних прав і свобод, плюралізму і незалежності виявлення поглядів, вільного обміну думками, ідеями та інформацією;
- духовна сфера стає критичною в умовах конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально-етичних цінностей. Так, проявом критичності духовної сфери (Ірландія, Алжир, Ізраїль, Афганістан, Китай, Іран) на міжнародному рівні стала проблема, пов'язана з рішенням керівництва ісламського

радикального руху «Талібан» (Афганістан) про руйнування неісламських релігійних пам'яток, що внесені до глобальної культурної спадщини і перебувають під охороною ЮНЕСКО [2, с. 61–62].

Відповідно до ст. 19 Закону України «Про національну безпеку України», Служба безпеки України є державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина:

1) протидію розвідувально-підривній діяльності проти України;

2) боротьбу з тероризмом;

3) контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, інформаційної безпеки держави, об'єктів критичної інфраструктури;

4) охорону державної таємниці.

Враховуючи викладене вище, необхідно зазначити, що в контексті визначених законом завдань, СБУ здійснює досить широке коло функцій, тим або іншим чином пов'язаних із забезпеченням інформаційної безпеки. До складу Центральне управління Служби безпеки України, яке відповідає за стан державної безпеки, координує і контролює діяльність інших органів Служби безпеки України, окрім інших, входять: функціональний підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, а також захисту державної таємниці.

Стратегією інформаційної безпеки на Службу безпеки України у межах компетенції покладено:

– моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері;
– протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [3].

Означені вище завдання, визначені Стратегією інформаційної безпеки, набувають особливого значення в умовах триваючої повномасштабної агресії, оскільки запорукою її продовження, окрім іншого, є успіхи в частині проведення інформаційних спецоперацій як в Україні, так і за її межами, з метою виправдання агресивних дій представників держави-агресора, а також псевдообгрунтування начебто дій України, які створили підґрунтя для повномасштабного вторгнення та анексії й окупації території України, що йому передувало.

Відповідно ж до п. 3 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки.

Також Служба безпеки України є спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці, виконуючи в цій сфері досить широкий спектр функцій.

Беручи до уваги сукупність суб'єктів, які забезпечують інформаційну безпеку, та сукупність їх завдань, прав і повноважень, можна відзначити, що існуюча система, навіть створена до початку повномасштабного вторгнення, проте така, що протидіяла активним заходам спецслужб рф, довела свою ефективність та здатність протистояти небезпечному ворогу. Разом

з цим необхідно відзначити, що на рівні керівних документів, які визначають перелік сучасних загроз, не було внесено жодних змін, які б відображали реалії сьогодення. Деякі проблемні питання вирішувались шляхом криміналізації діянь, що посягають на інформаційну складову воєнної безпеки та на інформаційну безпеку в цілому. Проте таких заходів очевидно недостатньо, оскільки зміни в керівних документах потягнуть за собою зміни архітектури завдань та цілей, спрямованих на їх вирішення, що, безперечно, активізує окремі складові забезпечення інформаційної безпеки.

Підводячи певний підсумок результатам проведеного аналізу в частині організаційно-правових засад забезпечення Службою безпеки України інформаційної безпеки держави в умовах воєнного стану, визначимо декілька висновків. По-перше, еволюція форм, методів та засобів шкідливого впливу на окремі складові інформаційної безпеки завжди випереджає еволюцію нормативно-правових та організаційних форм протидії, з огляду на що аналітична та прогностична діяльність по виявленню та виробленню дієвих форм протидії майбутнім загрозам набуває важливого стратегічного значення. По-друге, за відсутності дієвого стратегічного бачення поступового формування механізму забезпечення інформаційної безпеки в умовах повномасштабної збройної агресії доводиться лише в оперативному режимі закривати уразливості в існуючому механізмі, що завжди супроводжується завданою шкодою, переважно воєнній та державні безпеці нашої держави. По-третє, вбачається за доцільне посилити аналітичну діяльність з метою виявлення уразливостей в механізмі захисту інформаційної безпеки держави-агресора не лише в контексті воєнної безпеки рф, але й у інших сферах та складових її національної безпеки для можливості завдання шкоди не лише тактичного чи оперативно-тактичного рівня, але й стратегічної.

Список використаних джерел:

1. Конституція України, Закон від 28.06.1996 № 254к/96-ВР. Редакція від 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80. (дата звернення 17.06.2024)

2. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків: 2018. С. 61–62.

3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021 від 28.12.2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. (дата звернення 17.06.2024)

ПРОТИДІЯ ШАХРАЙСТВУ, ЩО ВЧИНЯЄТЬСЯ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Ірина СЕВРУК
аспірантка науково-дослідної лабораторії
з проблем протидії злочинності ННІ № 1
Національної академії внутрішніх справ

З поширенням Інтернету, розвитком інформаційних технологій та запровадженням процесів діджиталізації у всі сфери життя та суспільства загалом виникають (з'являються) нові можливості для отримання прибутку. Проте поряд із позитивними аспектами впровадження мережі «Інтернет» і стрімкого розвитку цифрових технологій міжнародна спільнота зіткнулася зі збільшенням кількості кіберзлочинів. За оцінками міжнародних експертів, щорічно за останні пять років майже 60% усіх вчинених кіберзлочинів були Інтернет-шахрайствами, від яких глобальні фінансові втрати сягають близько 55 мільярдів доларів щороку [1].

За оцінками спеціалістів український сегмент мережі Інтернет розвивається динамічно та у середньому за кожні шість місяців кількість збільшується в 1,7 разів. За кількістю провайдерів послуг Інтернет Україна знаходиться на першому місці серед країн Східної Європи [2]. З урахуванням глибокого проникнення мережі Інтернету в різні української сфери суспільної діяльності (банківська діяльність, телекомунікації, фінансова діяльність, торгівля та інші галузі) та його стратегічної ролі у проведенні банківських операцій, як засобу здійснення розрахунків (оплати), а також використання, як інструменту для зв'язку, заробітку, спілкування з друзями і близькими людьми та обміном інформацією через телефон, планшет, комп'ютер та ноутбук, проблема шахрайства, що вчиняється з використанням мережі Інтернет в Україні стала дефініційованою в сфері кібербезпеки та ідеальною платформою для діяльності організованих груп та злочинних організацій.

Виклики сьогодення, що спрямовані на значне збільшення шахрайства, що вчиняється з використанням мережі Інтернет є тісно пов'язані з пандемією Covid-2019 спричиненою коронавірусом, SARS-CoV-2, що розпочалася з 2019 року, а з 2022 року у зв'язку із військовою агресією російської федерації, що поєднане із повномасштабним збройним вторгненням рф на територію України під час яких жертвами шахраїв стали понад 11% українців [3]. Дохід шахраїв у лише 2023 році виріс на 201%, порівнюючи з 2022 роком і вперше перевищив позначку у мільярд. 2,9 млрд. [4].

Наразі шахрайство в Інтернеті набуває все більших масштабі. Саме анонімність шахраїв, відсутності безпосереднього контакту з потерпілим та масовість користувачів привертає значну увагу до мережі Інтернет шахраїв. Утім, види, способи, схеми та методи шахрайств дедалі удосконалюються, що значно ускладнює процес виявлення та документування і впливає на організаційно-тактичне забезпечення їх розслідування. Проведеним дослідженням встановлено основні проблеми, що виникають під час протидії органами Національної поліції України шахрайству, що вчиняється з використанням мережі Інтернет: високий рівень латентності, значна кількість та різноманітність способів вчинення Інтернет-шахрайств (79%); не достатність знань та вмінь в сфері інформаційно-аналітичного забезпечення (комп'ютерних технологій), кібернетики (75%); транснаціональних характер окремих випадків (75%); брак розробленої методики протидії (виявлення, документування та розслідування) шахрайству, що вчиняється з використанням мережі Інтернет (73%); невчасне проведення ОРЗ, СРД, НСРД та інших процесуальних заходів – (61%); відсутність впровадження ефективного досвіду інших країни щодо використання новітніх технічних засобів та програм під час виявлення таких злочинів (57%); відсутність злагодженої взаємодії (55%); наявність прогалин і недоліків в чинному законодавстві, а також відмінності в судових системах різних країн (55%); незадовільне фінансове та матеріально-технічне забезпечення (39%); неналежний обмін інформацією між правоохоронним органами (37%), а також інші несприятливі фактори, що значно знижує ефективність слідчої та оперативно-розшукової практики.

Згідно зі статистичними даними та офіційними звітами Офісу Генерального прокурора і Національної поліції України, встановлено, що кількість кримінальних правопорушень у сфері інформаційних технологій постійно зростає, упродовж 2019–2023 рр. виявлено (викрито) 58,7 тис. фактів шахрайства, що вчиняється з використанням мережі Інтернет (ч. 3, 4 ст. 190 КК України), з помітними тенденціями зростання динаміки вчинення даних кримінальних правопорушень, починаючи з: 2020 р.– у 1,8 разів (з 0,8 тис до з 1,4 тис), 2021– у 2 рази (з 1,4 тис до 2, 9 тис), 2022 р.– у 2,8 рази (з 2,9 тис. до 7,9 тис.), 2023 р.– у 5,8 рази (із 7,9 тис. до 45,7 тис.) [5]. Опитуванням працівників оперативних підрозділів НП Украйни встановлено, що такі кримінальних правопорушень, характеризуються: високим рівнем латентності (89%), внаслідок чого значна кількість фактів залишаються невикритими; організованим (88%) та професійним характером вчинюваних діянь (87%), незначною кількістю притягнутих до відповідальності, що на сьогодні залишається досить на низькому рівні (79%). Наведені статистичні дані та опитування свідчать про недостатню ефективність засобів і методів, що використовуються органами Національної поліції України під час протидії шахрайству, що вчиняється з використанням мережі Інтернет.

Встановлено, що Інтернет використовують як засіб здійснення розрахунків (оплати) (89%) та спосіб (спосіб готування, вчинення та приховування даного злочину) (91%) вчинення шахрайства через мережі Інтернет, а також під час вчинення даного злочину використовуються усі можливі інструменти для зв'язку із жертвами: телефон, Інтернет й електронна пошта. Аналіз слідчо-судової практики правоохоронних органів дає підстави виокремити найбільш поширені (найпопулярніші) типи (схеми, сценарії), які пов'язані із шахрайськими діями, що вчиняється з використанням мережі Інтернет (використання інформаційних технологій на різних стадіях): втрата документів, дзвінок від «працівника банку» (служби безпеки банку), з Вашим родичем «сталася біда» (родич у поліції або у лікарні); оренда нерухомості або товарів; «Перемога» в акції (Виграш) (під час онлайн-гри; псевдолотереї; спорт-прогнози, з лотереями/призами); сплата членського внеску, фальшивий чек, пов'язане з працевлаштуванням або туристичними послугами (виїзд за кордон); помилкове (випадкове) поповнення мобільного телефону, позичання грошей без наміру повернути борг, знайомства в Інтернеті (зловживання співчуттям), фіктивні шлюбні відносини («шлюбна афера»), фіктивні шлюбні агенції, нігерійські листи («листи щастя»); обіг криптовалюти; надання державних компенсаційних виплат; прохання знайомих про допомогу в соціальних мережах; акції або за заниження ціни на будь-які товари або речі; продаж або пропозиція доставки за низькою ціною автомобілів з закордону; проханнями про матеріальну допомогу для лікування; оплата посередницьких послуг; всілякі комерційні електронні операції щодо послуг: цифрового телебачення мобільного зв'язку або Інтернету; схеми швидкого збагачення (ділові пропозиції із завищеною оцінкою очікуваного прибутку; пільгові позики; інвестиційні піраміди); оплата онлайн-квитків (авіа-, залізничного та авто- призначення); продаж квітів, оптова закупка (8 Бререзня); шахрайства у сфері волонтерської діяльності та благодійної допомоги (збирання пожертвувань); пропонування віддаленої роботи, з перерахуванням початкового вкладу; купівля або продаж товарів через Інтернет у соціальних мережах (онлайн-шопінг). Окремо слід виокремити типи (схеми, сценарії), які пов'язані із шахрайськими діями, що вчиняється з використанням мережі Інтернет у зв'язку із збройною агресіює росії: збір коштів для військових; ваші рідні безвісти зникли або потрапили у полон; повідомлення про евакуаційний рейс за умови передплати; фейкова фінансова допомога під час війни (організація добровольчих або благодійних внесків, зокрема для тих постраждав від війни), допомога щодо виїзду за кордон, а також псевдовідкуп від армії (допомога в ухиленні від від військової служби та мобілізації). Констатовано, що види, типи (схеми) та способи шахрайських дій що вчиняється з використанням мережі Інтернет здійснюються у всіх сферах суспільства, а також постійно пристосовуються до ситуації та розвитку інформаційних технологій.

Установлено, що під час протидії органами Національної поліції України шахрайству, що вчиняється з використанням мережі Інтернет, відповідні підрозділи, взаємодіють: з прокурорами Офісу Генерального прокурора, Службою безпеки України (Департамент спеціальних телекомунікаційних систем та захисту інформації), Департаментом бюро розслідування, Бюро економічної безпеки України, Національним банком України (працівниками служб безпеки банків), Державною службою спеціального зв'язку та захисту інформації України, Державним центром кіберзахисту, урядовою командою реагування на комп'ютерні надзвичайні події України (далі CERT-UA), спеціалістами з комп'ютерної техніки, Інтернет-провайдерами, передовими IT-компаніями, кредитно-фінансовими установами, Державною службою фінансового моніторингу України, Державною пенітенціарною службою України, Державною кримінально-виконавчою службою, Державною фіскальною службою України, Державною прикордонною службою України, органами місцевої влади і самоуправління, адміністраціями і власниками підприємств та організацій, судами, засобами масової інформації громадськістю (окремими громадянами), спеціальними міжнародними органами та організаціями (ЄС, НЦБ Інтерпол, Європол, Європейським центром з розслідування кіберзлочинів (European Cybercrime Centre, ECC), Європейська служба зовнішніх справ (European External Action Service) Європейська агенцією мережевої та інформаційної безпеки (European Network and Information Security

Agency, ENISA), Група з реагування на комп'ютерні надзвичайні ситуації для установ, органів та установ ЄС (CERTEU), Європейська агенцією оборони (European Defence Agency), Консультативна місія Європейського Союзу (EUAM) та правоохоронними органами інших країн у рамках міжнародного співробітництва.

Список використаних джерел:

1. Шахрайство в Інтернеті. URL: https://kidslox.com/ua/guide-to/online-scams/.
2. Український сегмент мережі Internet сегодня. URL: http://boy.dlab.kiev.ua/PRJ/B_Intt/Main/Addon/Lib/anal_ukr/htm. (дата звернення 20.06.2024)
3. Кількість справ про шахрайство побила 12-річний рекорд. URL: https://delo.ua/society/kilkist-sprav-pro-saxraistvo-pobila-12-ricnii-rekord-431349/.(дата звернення 20.06.2024)
4. 3 млрд. грн склав «дохід» шахраїв у 2023 році – дослідження. Офіційне видання Delo.ua URL: https://delo.ua/war/rosiya-vdarila-po-objektu-televiziinoyi-infrastrukturi-v-xarkovi-jepereboyi-iz-signalom-431449/.(дата звернення 20.06.2024)
5. Про результати боротьби з організованими групами та злочинними організаціями. Офіс Генерального прокурора України. URL: https://gp.gov.ua/ua/posts/pro-rezultati-borotbi-z-organizovanimi-grupami-ta-zlochinnimi-organizaciyami-2. (дата звернення 20.06.2024)

ВИКОРИСТАННЯ МЕСЕНДЖЕРІВ ТА КРИПТОМЕСЕНДЖЕРІВ В ЗЛОЧИННІЙ ДІЯЛЬНОСТІ

Олексій СТАРОСТІН
старший викладач Національного юридичного
університету імені Ярослава Мудрого

Широке поширення Інтернету та радіорухомого стільникового зв'язку, зростання популярності мобільних пристроїв, наявність можливості застосування гнучкого, доступного якісного зв'язку на тлі постійного вдосконалення технічних методів і засобів його забезпечення, зумовили зміщення попиту населення від використання традиційного стільникового голосового зв'язку в бік так званих месенджерів (Telegram, WhatsApp, Viber, Signal, Threema та ін.). Схожа ситуація простежується в організації злочинної діяльності, підготовки та вчинення протиправних діянь.

В нормах чинного законодавства відсутнє пряме тлумачення поняття «месенджер». Позиція законотворця зводиться до того, що під месенджерами необхідно розуміти «платформи спільного доступу до інформації» – сервіс, що забезпечує своїм користувачам за їхнім запитом можливість зберігання та поширення користувацької інформації для необмеженого кола осіб, якщо такі зберігання та поширення не є незначною та суто допоміжною функцією іншого сервісу і з об'єктивних і технічних причин не може використовуватися без такого сервісу.

Щодо провайдерів платформ спільного доступу до інформації у ЗУ «Про медіа» немає окремої статті, адже вони не є суб'єктами регулювання закону. Їхня згадка в законі обмежується лише можливістю співпраці з державним органом.

Використовувані населенням України месенджери є програмними продуктами іноземного виробництва. Різниця в правових підходах помітно ускладнює питання регулювання використання закордонних месенджерів на території України, ідентифікації їхніх користувачів, визначення місць зберігання даних, що генеруються месенджерами, дешифрування трафіку, деанонімізації користувачів месенджерів, що функціонують у режимі обходу блокування за допомогою використання різних VPN-сервісів тощо.

На сьогодні залишається незрозумілою методика віднесення месенджера до «платформи спільного доступу до інформації». Це питання потребує обговорення і вирішення, тому що

зараз, спираючись на законодавче формулювання, неможливо визначити, що є месенджером у традиційному розумінні, оскільки чат у комп'ютерній онлайн-грі, чат-помічник, листування в різних додатках, онлайн-форумах, прямих трансляціях тощо також формально можна віднести до поняття «месенджер». Методика визначення поняття «месенджер» має узгоджуватися з потребами правозастосовної практики.

На тлі правової неврегульованості окреслених аспектів доводиться констатувати, що, крім користі для суспільства, месенджери знайшли активне застосування у протиправній діяльності. Наразі вони широко використовуються під час підготовки та скоєнні різних видів злочинів екстремістської та терористичної спрямованості, безконтактного збуту наркотичних засобів і психотропних речовин, дистанційного шахрайства та інших високоорганізованих злочинів. Месенджери використовуються як засоби обміну інформацією, інструменту керівництва діями членів злочинної групи під час підготовки та вчинення злочинів тощо. Частково такий попит пояснюється тим, що розробники імпортних месенджерів заявляють про високий ступінь шифрування і кодування повідомлень, які передаються, а це, в свою чергу, не дає змоги кому б то не було знайомитися з їхнім вмістом, а також високим рівнем анонімізації особистості користувачів додатків.

Така ситуація накладає істотний відбиток на організацію і тактику оперативно-розшукової діяльності, оскільки розвиток інтернет-технологій істотно видозмінює сформовані традиційні підходи до вирішення завдань боротьби зі злочинністю. Оперативно-розшуковими органами постійно удосконалюється практика застосування методів і засобів деанонімізації користувачів месенджерів; добування оперативно значущої інформації за допомогою використання метаданих та інформації про IP-адреси; встановлення даних користувачів під час реєстрації та авторизації в месенджерах.

Необхідно констатувати високий рівень обізнаності криміналітету про подібні заходи, що вживаються оперативно-розшуковими органами, зокрема про можливості картування генерованих метаданих, аналіз яких сприяє встановленню особи користувачів, фактичного місцеперебування тощо.

Подібні оперативно-розшукові заходи зумовлюють удосконалення механізму вчинення протиправних діянь, у тому числі зокрема за допомогою використання технічних новинок у сфері забезпечення комунікацій. Особливим попитом у злочинній діяльності стали користуватися засоби та методи забезпечення зв'язку з максимальним рівнем наскрізного шифрування, що не потребують реєстрації, автентифікації та ідентифікації під час використання застосунків і переважно безоплатного програмного забезпечення, що характеризуються відсутністю механізму збору та місць зберігання метаданих, які генеруються під час використанні месенджерів, та ін.

На сьогодні затребуваність у кримінально налаштованих осіб набули програмні рішення у вигляді мобільних додатків-месенджерів, які функціонують на основі використання децентралізованих однорангових самоорганізованих mesh-мереж, іншими словами, криптомесенджери (mesh-месенджери). Подібний інтерес обумовлений технічними особливостями функціонування цих мобільних додатків, які в сукупності здатні забезпечити максимальний ступінь шуканої криміналітетом приватності та анонімності, відсутність цифрових слідів. Основною відмінністю криптомесенджерів від звичайних месенджерів заведено вважати децентралізований принцип роботи, відсутність метаданих і серверів зберігання інформації. Таке стало можливим завдяки використовуваній у криптомесенджерах технології Mesh Networks (у перекладі з англ. сітчасті мережі), суть якої полягає в побудові самоорганізованої архітектури мережі, що має такі ознаки:

– функціонування криптомесенджерів без підключення до ресурсів стаціонарного та мобільного Інтернету, стільникового зв'язку;
– наявність можливості безперешкодної незалежної побудови мережі, де людина за наявності достатньої кількості мобільних пристроїв зі встановленими відповідними додатками здатна організувати свою мобільну мережу для передавання різних даних;

– створення мобільної зони покриття з можливістю її переміщення у просторі;
– використання бездротових каналів зв'язку стандартів мобільної зони покриття з можливістю її переміщення в просторі;
– використання бездротових каналів зв'язку стандартів IEEE Wi-Fi (802.11 – для локальних і міських мереж), Bluetooth (IEEE 802.15.1 – для побутових пристроїв), ZigBee (IEEE 802.15.4 – для датчиків);
– застосування принципу поєднання маршрутизаторів і ретрансляторів, коли кожен вузол або станція приймає повідомлення та одночасно перенаправляє їх іншому адресату (іншими словами, у випадках вимкнення однієї зі станцій мережі (у нашому випадку це мобільний пристрій у вигляді смартфона або планшета) інші станції, під'єднані до такої мережі, продовжують функціонувати, забезпечуючи з'єднання між собою напряму або через проміжні вузли з автоматичним переналаштуванням мережі);
– відсутність серверів і центрів обробки даних, а також метаданих використання криптомесенджерів.

Закордонна практика вказує на наявність фактів застосування криптомесенджерів (Firechat, Bridgefy, Signal Offline Messenger та ін.) при вирішенні різних кримінальних завдань, в основному як засіб обміну інформацією під час проведення протестних акцій і громадських заворушень.

Вказана ситуація поставила перед правоохоронними органами складні для розв'язання завдання в частині отримання оперативно значущої інформації, коли фактично при використанні криптомесенджерів відсутні можливості здійснення перехоплення трафіку, встановлення особи користувача такої мережі за метаданими або за інформацією з серверів розробника тощо.

Обмежити можливість використання подібних бездротових технологій фізично не є можливим з огляду на масштаби їх застосування. Наразі практично будь-який мобільний пристрій (стільниковий телефон, планшет, ноутбук), інші технічні засоби зв'язку обладнані вузлами Wi-Fi та Bluetooth.

Чинні норми законодавства у сфері зв'язку зобов'язують реєстрацію у відповідних органах засобів зв'язку, інших радіоелектронних засобів і високочастотних пристроїв, які є джерелами електромагнітного випромінювання, за винятком пристроїв малого радіусу дії, до числа яких належить більшість побутових мобільних пристроїв зв'язку, навігації тощо. Правоохоронним органам доводиться здійснювати пошук ефективних форм і методів протидії застосування криптомесенджерів у злочинній діяльності за допомогою адресного використання апаратно-програмних засобів придушення сигналу Wi-Fi та Bluetooth. Паралельно правоохоронним органам необхідно здійснювати комплекс заходів щодо ідентифікації користувачів криптомесенджерів, добування та вилучення оперативно значущої інформації з мобільних пристроїв, що використовують криптомесенджери.

Що стосується заходів з ідентифікації користувачів криптомесенджерів, добування та вилучення оперативно значущої інформації з мобільних пристроїв, слід звернути увагу на те, що правоохоронним органам необхідно використовувати наявні сили, засоби та методи в сукупності. Комплексний підхід передбачає застосування білінгових даних операторів стільникового зв'язку, інформації, витягнутої з мобільних пристроїв, з біометричних баз даних, отриманої за допомогою камер відеоспостереження та ін.

В Україні, з метою отримання електронних доказів кримінальних правопорушень, законодавством передбачена практика виявлення та вилучення мобільних пристроїв. В першу чергу, у таких випадках, намагаються вилучити мобільний пристрій не в заблокованому вигляді або під час виконання власником мобільного пристрою лише вихідного дзвінка, а також попередити можливість шифрування пристрою. У разі вилучення мобільного пристрою із заблокованим екраном роблять усе можливе, аби не дати його вимкнути. Також проводяться заходи щодо запобіганню видаленню інформації віддаленим способом.

Це ж саме стосується і комп'ютерної техніки, так як більшість популярних месенджерів мають десктоп-версії.

Список використаних джерел:

1. Про медіа: Закон України від 13 грудня 2022р. № 2849-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2849–20#Text. (дата звернення: 15.05.2024)
2. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992р. № 2135-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2135–12#Text. (дата звернення: 15.05.2024)
3. Кримінальний кодекс України від 05 квітня 2001р. № 2341-III / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text. (дата звернення: 15.05.2024)
4. EUNEWS. Europe's police forces united against encrypted messaging: «It will prevent us from investigating the most serious crimes». URL: https://www.eunews.it/en/2024/04/22/europes-police-forces-united-against-encrypted-messaging-it-will-prevent-us-from-investigating-the-most-serious-crimes/. (дата звернення: 10.05.2024)

ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ ПОКОЛІННЯ 5G

Юрій ЧЕЛПАН
співробітник СБУ
Валерій СТЕПАНОВ
кандидат технічних наук,
співробітник СБУ

Оперативним підрозділам для виконання завдань оперативно-розшукової діяльності при наявності відповідних підстав надається право на зняття (законне перехоплення) інформації з електронних комунікаційних мереж [1].

Постачальники послуг електронних комунікацій в Україні розпочали впровадження технології мобільного зв'язку п'ятого покоління 5G. Відмінності технології 5G від технологій 3/4G викликають необхідність перегляду підходів щодо законного перехоплення інформації в мережах мобільного зв'язку покоління 5G.

В статті [2] зазначені основні підходи щодо законного перехоплення інформації в мережах мобільного зв'язку покоління 3/4G.

По-перше, застосування єдиної системи технічних засобів, що зазначена в пункті 2 статті 121 Закону України [3], загальні вимоги до якої наведені в нормативному документі [4]. Технічні засоби єдиної системи взаємодіють за стандартизованими інтерфейсами з технічними засобами електронних комунікаційних мереж (як правило, зі шлюзами мережних комплектів та/або серверами, що виконують посередницькі функції під час взаємодії з комутаційним обладнанням, вузловими шлюзами мережі, регістрами місцезнаходження, серверами абонентських даних, тощо). Функція законного перехоплення інформації (Lawful Interception) в мережах мобільного зв'язку покоління 5G стандартизована Партнерським проектом третього покоління (3GPP) та Європейським інститутом телекомунікаційних стандартів (ETSI).

В цьому підході слід врахувати появу в мережі 5G нових ознак об'єктів перехоплення (ідентифікаторів): SUPI (subscriber permanent identity), GUTI (globally unique temporary identity), SUCI (subscription concealed identifier), PEI (permanent equipment identifier), GPSI (generic public subscription identifier), під час формування таблиці спостереження. Додатково необхідно організувати взаємодію з новими функціональними модулями (обладнанням відбору об'єктів перехоплення) ядра мережі 5G (5G Core Network), до яких необхідно віднести наступні модулі:

– AMF (core access and mobility management function) – мережної функції управління доступом та мобільністю;

– SMF (session management function) – мережної функції управління сеансами користувачів послуг;
– UDM (unified data management) – управління даними користувачів послуг на основі уніфікованої бази даних його профілів;
– SMSF (SMS function) – функції підтримки обміну короткими текстовими повідомленнями через протокол NAS;
– UPF (User Plane Function) – функції площини передачі даних користувачів послуг;
– NEF (network exposure function) – функції забезпечення взаємодії з зовнішніми платформами та додатками.

По-друге, застосування стаціонарних комплексів активної дії для зняття інформації з електронних комунікаційних мереж мобільного зв'язку. Вказані комплекси відгалужують інформацію щодо обміну даними між функціональними модулями мережі, в інтерфейсах взаємодії яких відсутні механізми шифрування даних.

Ядро мережі 5G Core, підтримує криптографію TLS (Transport layer security). В мережах 5G для реалізації вказаного підходу необхідно, щоб постачальник послуг примусово вимкнув шифрування протоколу TLS. В подальшому оперуючи отриманими даними здійснюється відгалуження інформаційних повідомлень та/або службових даних сеансів зв'язку абонентів спостереження, інформація щодо їх місцезнаходження та закріплений профіль послуг.

По-третє, застосування мобільних комплексів активної дії для зняття інформації з електронних комунікаційних мереж мобільного зв'язку. Вони використовують підроблені (несправжні) базові станції для обслуговування абонентів спостереження (споживачів послуг) та, як слід, перехоплення їх сеансів зв'язку.

В цьому підході слід врахувати появу в мережі 5G нових асоціацій ідентифікаційних ознак об'єктів перехоплення SUCI з SUPI та 5G-GUTI з SUPI.

У додатку Г нормативного документа [4] зазначено про необхідність надання постачальниками електронних комунікаційних мереж та/або послуг до засобів управління системою перехоплення уповноваженого органу службових даних електронних комунікацій та збережених ними протягом строку позовної давності, визначеного законом, записів про надані комунікаційні послуги.

Зазначену вище інформацію, в тому числі асоціації ідентифікаційних ознак об'єктів перехоплення SUCI з SUPI та 5G-GUTI з SUPI необхідно використовувати в комплексах активної дії для формування таблиць спостереження.

По-четверте, застосування мобільних комплексів пасивної дії для зняття інформації з електронних комунікаційних мереж мобільного зв'язку шляхом перехоплення та за необхідності дешифрування інформації, що циркулює в інтерфейсах обміну інформації між кінцевим (термінальним) обладнанням та базовими станціями та/або ретрансляторами сигналів, що входять до складу мережної інфраструктури.

В цьому підході слід врахувати появу в мережі 5G нових асоціацій ідентифікаційних ознак об'єктів перехоплення SUCI з SUPI та 5G-GUTI з SUPI для формування таблиць спостереження.

Висновки та перспективи.

Під час дослідження підходів щодо законного перехоплення інформації в мережах мобільного зв'язку покоління 5G визначено низку проблемних питань та запропоновані механізми їх реалізації.

Викладений у тезах матеріал рекомендуємо використовувати під час підготовки нормативно-правових актів та нормативних документів у сфері законного перехоплення, а також в подальшому для планування оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах мобільного зв'язку 5G.

Список використаних джерел:

1. Про оперативно-розшукову діяльність : Закон Країни від 18.02.1992 № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303.

2. Степанов В.А., Грищенко С.М. Технічні засоби для негласного зняття інформації з електронних комунікаційних мереж. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2021. № 4 С. 279–283.

3. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. Офіційний вісник України. 2021. № 6 (20.06.2024). Ст. 306.

4. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій в електронних комунікаційних мережах загального користування України. Загальні технічні вимоги: Наказ Служби безпеки України і Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 31.12.2021 року № 460/781. URL: ssu.gov.ua/uploads/documents/2022/01/24/ztv- 31122021.pdf (дата звернення 12.06.2024).

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАБЕЗПЕЧЕННІ ДЕРЖАВНОЇ БЕЗПЕКИ

Євген ЧЕРНЕНКО
співробітник СБУ

Стрімкий розвиток технологій штучного інтелекту в останні роки призвів до появи масово доступних інструментів аналізу та генерації великих масивів даних. Крім того, в державах з розвиненим ІТ сектором ведуться розробки продуктів, які не доступні широкому загалу. Інформаційні процеси прискорюються, а зростання кількості контенту, який не контролюється державою вимагає адекватної та оперативної відповіді для забезпечення державної безпеки. Враховуючи це, державні інституції мають самі брати на озброєння системи штучного інтелекту, як високоефективні інструменти обробки інформації, та приймати регуляторні нормативно-правові акти для мінімізації ризиків та загроз, які можуть виникати при створенні та використанні систем штучного інтелекту.

Можливості штучного інтелекту можуть бути використані як для захисту від загроз державній безпеці, так і для активних дій в інформаційному просторі ворога.

Перерахуємо декілька варіантів застосування технологій ШІ в контексті забезпечення державної безпеки:

1. Аналіз великих масивів даних для ідентифікації та реакції на інформаційні впливи ворога.

2. Генерація наративів для впливу на когнітивний простір цільової аудиторії.

3. Первинний контррозвідувальний пошук.

Найбільш відомим прикладом аналізу великих масивів даних для протидії російським інформаційним впливам є розробка команди українського стартапу Mantis Analytics, яка після початку широкомасштабного вторгнення створила свій продукт і почала співпрацювати з РНБО України. Розробка команди допомагає виявити дезінформацію та швидко прийняти рішення, як їй протидіяти. На реакцію, після виявлення вкиду, відводиться до 24 годин. Якщо працювати вручну, відреагувати у такий короткий проміжок складно – перед цим інформацію треба зібрати, обробити, проаналізувати та верифікувати результати. В умовах, коли лише в одному Telegram генеруються терабайти інформації, без технологій ШІ не обійтися.

Працює це наступним чином. До системи завантажується масив даних (наприклад, повідомлення та коментарі з понад сотень тисяч каналів в Telegram). Штучний інтелект обробляє їх та проводить очищення від нерелевантної інформації та розподіляє на два потоки: фізичні події та ментальні сигнали. NLP (обробка природної мови) та LLM (велика мовна модель)

застосовують свої аналітичні здібності, щоби виявити потенційну дезінформацію, пропагандистські техніки, просканувати настрої в інформаційному полі та геокодувати джерела або події. Система ставить оцінку потенційно небезпечним повідомленням та сповіщає про них. Додатково результат можуть верифікувати «вручну». [1].

Такий метод обробки даних дозволяє виконувати роботу з відстеження інформаційних потоків в реальному часі, а також створити мапу інформаційного впливу (інформаційний простір) для відстеження реакцій та поведінки населення, напрямків та джерел інформаційного впливу.

Для ефективного впливу на когнітивний простір, мають враховуватися ідентичності цільових аудиторій. Тому потребується створення мапи ідентичностей, які мають формуватися шляхом перепису населення, соціологічних досліджень та інформаційно-аналітичних досліджень СБ України та інших державних інституцій.

Введення такого масиву даних до системи штучного інтелекту дозволить генерувати наративи, в тому числі і стратегічний, стосовно різноманітних подій та фактів для різних рівнів. Глобального – має бути спрямований на найширшу аудиторію, враховуючи фактори культурної, релігійної, расової, національної різноманітності, з акцентом на загальнолюдські цінності, внесок і роль України в їх реалізацію. Державного – має бути спрямований на аудиторію всієї держави (будь-якої, в межах одного інформаційного простору), в залежності від цілей і національних інтересів. Регіонального – має бути спрямований на аудиторію в межах певного регіону держави (географічного, етнічного, релігійного, ін.). Локального – має бути спрямований на певну спільноту, в межах невеликої територіальної громади. Індивідуального – має бути спрямований на окремих осіб в залежності від їхніх ідентичностей (професійна, вікова, етнічна, релігійна та інші).

Домінування у когнітивному просторі є критично важливим з точки зору вербувальної вразливості. Практика доводить, що вербування на основі добровільної згоди дає кращі результати, ніж примус, бо мотиви агента до розвідувальної діяльності співпадають з його внутрішніми мотивами, заснованими на власній ідентичності.

Тому застосування високоефективних систем штучного інтелекту для формування суспільної та індивідуальної свідомості є перспективним методом забезпечення інформаційної та когнітивної безпеки держави.

Що стосується застосування систем штучного інтелекту для первинного контррозвідувального пошуку, то їхні аналітичні здібності можуть застосовуватися для знаходження та ідентифікації потенційних агентів ворожих спецслужб через сканування дописів та коментарів у соціальних мережах та мессенджерах.

Враховуючи, що під час повномасштабного вторгнення спеціальні служби російської федерації почали масово використовувати соціальні мережі та мессенджери для віддаленого вербування, маючи аналітичну інформацію про потенційних агентів, сформовану системою штучного інтелекту, співробітники Служби безпеки України зможуть відкривати контррозвідувальні справи для здійснення додаткових гласних і негласних оперативних заходів. Окрім цього, може здійснюватися адресна профілактична розсилка повідомлень про відповідальність за державну зраду, колабораційну діяльність та інші злочини проти основ національної безпеки.

Тому, застосування технологій штучного інтелекту для забезпечення державної безпеки є необхідним елементом системи забезпечення національної безпеки у час війни, коли технологічна перевага є життєво важливим фактором протистояння ворогу із суттєво переважаючими ресурсами.

Список використаних джерел

1. Від пошуку російських фейків до захисту корпоративних активів в США. Історія українського стартапу Mantis Analytics. URL: https://journal.gen.tech/post/istoriya-ukrayinskogo-startapu-mantis-analytics. (дата звернення 15.06.2024).

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ

Анна ЯРОШ
кандидат юридичних наук,
співробітник СБУ

На сьогодні світ опинився перед новими викликами у сфері забезпечення інформаційної безпеки, яка в умовах глобалізації та інтеграції є ключовим чинником забезпечення спроможності країни долати кризові явища зовнішньої агресії. Нині Україна перебуває в стані війни, у тому числі й інформаційної війни, а тому все динамічнішими стають її зовнішні та внутрішні загрози, які спрямовані на руйнування національного суверенітету та територіальної цілісності України, пропагування ідеї сепаратизму, насильства, національної ворожнечі, що є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди. Отже, в умовах збройної агресії питання забезпечення інформаційної безпеки стають ще більш актуальними та своєчасними.

Серед вітчизняних авторів, які приділяли у своїх роботах значну увагу аспектам інформаційної безпеки у своїх роботах приділяли такі вітчизняні автори, як: І. Боднар, С. Гончар, В. Демиденко, В. Ліпкан, Л. Кочубей, В. Цимбалюк та ін.

Конституцією України в ст. 17 зазначено, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу [1].

У Стратегії інформаційної безпеки України інформаційна безпека розглядається як важливий елемент національної безпеки України, що гарантує захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [2].

Наукових визначень інформаційної безпеки існує сьогодні дуже багато, однак досі немає єдиної думки щодо її сутності. За класифікацією В. Ліпкана, можна виокремити декілька підходів до визначення сутності феномену інформаційної безпеки, за якими під останнім розуміють: стан захищеності інформаційного простору; процес управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; стан захищеності національних інтересів країни в інформаційному середовищі або в інформаційній сфері; захищеність установлених законом правил, за якими відбуваються інформаційні процеси в державі; важливу функцію держави; суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі; невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки [3, с. 25–30]. Вчений В.С. Цимбалюк вважає, що інформаційна безпека України це стан захищеності її національних інтересів в інформаційній сфері, який визначається поєднанням збалансованих інтересів особи, суспільства та держави [4, с. 18]. Заслуговує на увагу думка науковця Л.О. Кочубей, яка вважає, що інформаційна безпека характеризує стан захищеності життєво важливих інтересів, інформаційну озброєність держави, суспільства, особистості, за якої жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів [5, с. 221].

Отже, під інформаційною безпекою пропонуємо розуміти стан захищеності життєво важливих інтересів людини, суспільства і держави від протиправних інформаційних впливів.

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, насильницьку зміну конституційного ладу або порушення суверенітету і територіальної цілісності України.

Саме тому серед національних викликів та загроз, що постали перед Україною у зв'язку зі збройною агресією РФ Стратегія інформаційної безпеки визначає наступні:

– інформаційний вплив Російської Федерації як держави-агресора на населення України;
– інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України;
– обмежені можливості реагувати на дезінформаційні кампанії;
– спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України [2].

З метою попередження і протидії зазначеним існуючим та потенційним загрозам інформаційній безпеці завдання держави потягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Важлива роль у даному напрямі належить державним органам, які відповідно до наданих повноважень повинні здійснювати організаційне, нормативно-правове, матеріально-технічне та фінансове забезпечення реалізації державної політики у сфері інформаційної безпеки.

Серед ключових напрямів, які має виконувати механізм забезпечення інформаційної безпеки варто відзначити наступні: 1) технічний – тобто створення і функціонування всіх необхідних технічних складових систем (зокрема, створення і розвиток інформаційних систем; створення умов для якісного й ефективного інформаційного забезпечення; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій і засобів їх забезпечення); 2) політичний – державна політика повинна бути спрямована на забезпечення інформаційної безпеки (зокрема, визначення місця інформаційної безпеки в системі національної безпеки, розроблення пропозицій щодо вдосконалення інформаційного законодавства стосовно визначення інформаційних загроз та небезпек); 3) правовий – оформлення всіх пов'язаних елементів у якісні нормативно-правові акти з урахуванням сучасного зарубіжного досвіду забезпечення інформаційної безпеки.

Отже, питання забезпечення інформаційної безпеки набули особливої актуальності у зв'язку з появою нових викликів і загроз, спричинених збройною агресією РФ. Національні інтереси України у сфері інформаційної безпеки повинні полягати у розвитку сучасних телекомунікаційних технологій, у попередженні та протидії існуючим та ймовірним загрозам інформаційній безпеці, у прийнятті якісних нормативно-правових актів з урахуванням сучасного зарубіжного досвіду забезпечення інформаційної безпеки. У зв'язку з цим стратегічне завдання держави полягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки, що є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини.

Список використаних джерел:

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР Дата оновлення: 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. (дата звернення 18.06.2024)

2. Про рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021 Дата оновлення: поточна редакція. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. (дата звернення 18.06.2024)

3. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: [навчальний посібник]. К.: КНТ, 2006. 280 с.

4. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

5. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса. 2015. Вип. 3. С. 220–237.

КІБЕРВІЙНА: ВИКЛИКИ ДЛЯ СУДОВОЇ ЕКСПЕРТИЗИ, НОВІ ВИМІРИ СУЧАСНОГО КОНФЛІКТУ ТА ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Ілона ЯЦЕНКО
судовий експерт
Науково-дослідного центру судової експертизи
у сфері інформаційних технологій та
інтелектуальної власності
Міністерства юстиції України

Тривалий час Україна знаходиться в стані гібридної війни та стикається зі складними викликами в цифровому просторі. «Кібервійна» стала невід'ємною складовою сучасних конфліктів, вона відкриває нові виміри боротьби та потенційної шкоди для національної безпеки країни.

Український професор міжнародного права Мережко О.О. визначає кібервійну так: «кібервійна» – використання Інтернету й пов'язаних з ним технологічних і інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету іншої держави [1].

Наразі Міністерство оборони України активно працює над законодавчим визначенням поняття «кібервійна», що дасть можливість вивести поняття «кібервійна» у правове поле. Реалізація цього кроку на законодавчому рівні має важливе значення у протидії кіберзагрозам. З початку повномасштабного вторгнення фахівці Служби безпеки України нейтралізували майже 10 тисяч кібератак. Оскільки дії агресора в кіберпросторі є системними і направленими вже не лише на Україну, а і на її союзників, слідом за визначенням поняття «кібервійна» на національному законодавчому рівні, визнання кібератак як акту війни у правовому полі має також відбутися і на міжнародному [2].

У сьогоденні Україна постійно стикається зі спробами кібератак на важливі державні та комерційні інформаційні системи, які можуть мати серйозні наслідки для державної безпеки, економіки та громадської довіри. Україна стала мішенню для різноманітних кібератак, включаючи DDoS-атаки на урядові та військові вебсайти, шпигунство в кіберпросторі, а також спроби зламу критично важливих інформаційних систем. Напади на критично важливі інфраструктури, такі як енергетика, транспорт та телекомунікації, мають серйозні наслідки для функціонування країни та безпеки її громадян, тому Україна має вдосконалювати захист критично важливих інфраструктур від кіберзлочинності.

Визначення терміну «кібератака» наведено в Законі України «Про основні засади забезпечення кібербезпеки України». Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [3].

Судова експертиза в «кібервійні» відіграє важливу роль, зокрема у встановленні фактів, які допомагають судовим органам приймати обґрунтовані рішення у справах, пов'язаних з кібербезпекою та кіберзлочинами. Судова експертиза у «кібервійні» є необхідною та важливою в різних ситуаціях.

Одним з можливих викликів для судової експертизи у цьому контексті є виявлення хакерських атак, що є важливим аспектом для розслідування кіберзлочинів і забезпечення кібербезпеки Якщо відбулася кібератака на комп'ютерну систему або інформаційні ресурси, судова експертиза може допомогти виявити, як саме це сталося, які конкретно методи були використані зловмисниками.

Ключовими аспектами процесу хакерських атак є, зокрема:

– аналіз логів та журналів: експерти аналізують системні логи та журнали активності для виявлення незвичних або підозрілих дій. Це може включати спроби несанкціонованого доступу, зміни в системних налаштуваннях, спроби видалення або модифікації файлів, активність з надання привілеїв тощо. Історія системних подій дозволяє встановити час, тип і масштаб атаки;
– аналіз мережевого трафіку: шляхом аналізу мережевого трафіку експерти можуть виявити незвичні з'єднання, надмірну активність, спроби перехоплення даних або використання вразливостей мережевих протоколів. Важливо встановити шлях, яким проник зловмисник, і визначити масштаб його дій;
– дослідження вразливостей: експерти можуть провести аналіз системи на предмет виявлення вразливостей, які могли бути використані зловмисником для атаки. Це може включати перевірку патчів, оцінку конфігурацій системи та інші фактори, що можуть впливати на безпеку системи;
– аналіз коду та програмних засобів: за умови використання зловмисником спеціалізованих програмних засобів або злому коду експерти можуть аналізувати цей код для виявлення слідів діяльності зловмисника, включаючи використані техніки атаки та методи обходу захисту;
– реконструкція подій: на основі отриманих доказів / інформації експерти можуть відтворити послідовність подій, що призвели до інциденту.

Важливо, щоб усі отримані докази / інформація були задокументовані і збережені відповідно до вимог діючого законодавства.

Також судова експертиза є необхідною для аналізу цифрових доказів, таких як електронні листи, повідомлення, файли або журнали активності, щоб довести факти злочинів або порушень.

Цифрові докази в судовій експертизі включають у себе всі види електронних інформаційних матеріалів, які можуть бути використані для встановлення фактів, пов'язаних з правопорушенням.

Ключовими цифровими об'єктами судової експертизи є:

– електронні повідомлення, які можуть включати електронні листи (e-mails), текстові повідомлення (SMS), чати, повідомлення в соціальних мережах тощо;
– цифрові файли – документи, аудіо- або відеозаписи, фотографії, програмний код, електронні таблиці, презентації тощо. Ці файли можуть містити важливу інформацію для судових розслідувань, наприклад, контракти, фінансові звіти, документи тощо;
– цифрові журнали і логи – системні і апаратні журнали, які містять інформацію, зокрема про активність системи, включаючи дії користувачів, доступ до ресурсів, мережеву активність;
– метадані – інформація, яка додається до файлів, така як час і дата створення, зміни, відправлення або отримання, а також відомості про авторство чи власників файлів. Метадані є важливими для підтвердження автентичності документів або визначення послідовності подій.

Також в ситуаціях, коли виникає підозра на кібершпигунство або незаконне кіберпроникнення в комп'ютерні системи чи мережі, судова експертиза може визначити, зокрема які дані були вкрадені або змінені.

Судова експертиза може оцінити масштаб і наслідки кібератаки, включаючи фінансові збитки, втрату даних, порушення конфіденційності чи можливість втручання у критичні інфраструктурні системи.

Крім того, серйозні виклики в сучасному інтернет-середовищі представляють кібербулінг і кіберзлочини.

Кібербулінг є формою цифрового насильства, яке включає в себе використання електронних комунікаційних технологій, таких як соціальні мережі, текстові повідомлення, електронна пошта тощо, для систематичного заподіяння емоційної чи психологічної травми чи страждань. Під час здійснення судової експертизи, з метою встановлення фактів кібербулінгу, експерти аналізують електронні повідомлення, текстові записи, фотографії, відео, досліджують цифрові сліди, які залишаються після кібербулінгу, такі як історія переписки, дати та часи надсилання повідомлень, інформація про використані пристрої тощо.

В свою чергу кіберзлочини мають значно ширше поняття, що охоплює різноманітні протиправні / кримінальні діяння, які здійснюються через інформаційні технології. Сюди відносяться кібератаки, крадіжки особистих даних, шахрайства, дестабілізація мережевої безпеки тощо. У таких випадках експерти проводять дослідження, які включають аналіз мережевого трафіку, системних журналів, цифрових слідів та інших даних для виявлення підозрілих активностей. На основі отриманої інформації / даних експерти можуть реконструювати послідовність подій, які призвели до кіберзлочину, включаючи час та спосіб вчинення злочину.

Загалом, судова експертиза у «кібервійні» відіграє важливу роль у зборі об'єктивних доказів, встановленні важливих фактів та допомагає приймати обґрунтовані рішення у справах, пов'язаних з кібербезпекою та кіберзлочинами.

Оскільки кіберзахистом є сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямованих на забезпечення кібербезпеки [3], важливим аспектом захисту інформаційних ресурсів України також може стати і підвищення рівня кіберосвіти серед населення та підготовка кваліфікованих кадрів у галузі кібербезпеки – захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасного виявлення, запобігання і нейтралізації реальних і потенційних загроз національній безпеці України у кіберпросторі [3].

При цьому загальною стратегією захисту інформаційних ресурсів України є поєднання технологічних, організаційних та людських ресурсів з метою виявлення, запобігання та відповіді на кіберзагрози. Важливою складовою стратегії є постійна оцінка ризиків та адаптація заходів захисту до змін у кіберпросторі.

На мою думку, постійна та кропітка робота з розроблення, удосконалення вже існуючої стратегії щодо кіберзахисту, матиме позитивні наслідки захисту кіберпростору. Визначені стратегії мають бути не лише узгодженими та систематично впровадженими, але й постійно оновлюватися та адаптуватися до змін у кіберзагрозах та технологічних трендах.

Вважаю, що інвестиції в кібербезпеку та створення відповідних правових норм забезпечать надійну безпеку в цифровому просторі. Здійснення постійного моніторингу кіберпростору, з метою вчасного виявлення потенційних загроз та реагування на них, матиме ефективний результат. Застосування сучасних кібертехнологій, таких як шифрування, автентифікація, виявлення загроз та інших, допоможе створити надійні механізми захисту кіберпростору.

Не менш важливим етапом ефективної боротьби з кіберзлочинністю є співпраця з іншими країнами та міжнародними організаціями у сфері обміну інформацією про кіберзагрози та спільній розробці стратегій захисту.

Крім того, важливим етапом має стати підвищення рівня кіберосвіти серед населення та кадрового забезпечення державних інститутів у сфері кібербезпеки.

Зміцнення кіберпідготовки та освіти охоплює різні аспекти, від освіти населення до професійної підготовки фахівців у галузі кібербезпеки, адже люди повинні розуміти основні кіберзагрози, вміти визнавати підозрілі поведінки в Інтернеті, користуватися безпечними паролями

та захищати свої особисті дані. Інтеграція кібербезпеки у навчальні плани та програми допоможе молодому поколінню розвинути необхідні навички та усвідомлення щодо кібербезпеки ще на ранніх стадіях їх освітнього шляху. Створення програм навчання та сертифікації у галузі кібербезпеки допоможе забезпечити наявність кваліфікованих кадрів. Це включає в себе тренінги, курси, майстер-класи та інші форми навчання, які охоплять широкий спектр тем, від технічних аспектів кібербезпеки до управління ризиками та стратегічного планування.

Створення спеціалізованих центрів, лабораторій та інститутів, які зосередяться на дослідженнях та навчанні у сфері кібербезпеки, сприятиме розвитку інновацій та розробці нових методів захисту. Запрошення професіоналів з великим досвідом у сфері кібербезпеки для проведення лекцій, тренінгів та практичних занять допоможе студентам та фахівцям отримати відмінну підготовку.

Зміцнення кіберпідготовки та освіти вимагає систематичного підходу та співпраці між урядовими установами, освітніми закладами, приватним сектором та громадськістю.

Кіберосвітні програми у школах та університетах відіграють важливу роль у формуванні усвідомленості щодо кібербезпеки серед учнів та студентів. Ці програми можуть бути різноманітними, але орієнтовані на навчання учнів та студентів основам кібербезпеки, збільшення їх навичок у безпечному користуванні Інтернетом та виявленні потенційних кіберзагроз.

До прикладу, школи та університети можуть включати курси з кібербезпеки у свої програми навчання. Ці курси можуть охоплювати такі теми, як безпека в Інтернеті, захист від кібератак, етика в Інтернеті та інші аспекти цифрової безпеки. Учні та студенти можуть брати участь у різноманітних проектах та робочих групах, спрямованих на вивчення проблем кібербезпеки та розробку стратегій захисту, шляхом участі у змаганнях з кібербезпеки, проведенні досліджень у цій галузі та розроби протоколів безпеки. Практичні вправи та симуляції дозволять учням та студентам використовувати свої знання та навички у реальних сценаріях. Запрошення експертів з кібербезпеки для проведення гостьових лекцій та майстер-класів допоможе учням та студентам отримати інсайди з перших вуст, дізнатися про актуальні тренди у цій галузі та почути про практичний досвід роботи в сфері кібербезпеки. Використання інтерактивних ресурсів, відеоуроків, онлайн-гравців та ігор може зробити процес навчання цікавішим та змістовнішим для учнів та студентів.

Отже важливим є те, що відповідно до специфіки сучасного цифрового середовища і загроз, що випливають з нього, стратегії протидії кіберзагрозам мають бути комплексними та постійно адаптованими.

Загальна мета кіберосвітніх програм у школах та університетах має полягати в тому, щоб підготувати молоде покоління до викликів і загроз цифрового світу, розвинути у них критичне мислення та навички самозахисту в Інтернеті, а також створити базу для подальшого професійного розвитку у галузі кібербезпеки. Рішення зазначених проблем потребує комплексного підходу, який включає в себе розвиток кіберзахисту, підвищення кіберосвіти, зміцнення інформаційної безпеки критично важливих інфраструктур, підтримку незалежних медіа та активну міжнародну співпрацю.

В свою чергу складним та важливим завданням судової експертизи в захисті інформаційних ресурсів України є кропітка робота експертів з надання висококваліфікованих та об'єктивних висновків, які використовуватимуться як джерела доказів в нелегкому протистоянні країни у «кібервійні».

Список використаних джерел:

1. Кібервійна. URL: https://www.wikiwand.com/uk/Кібервійна (дата звернення: 11.06.2024).

2. Офіційний вебсайт Міністерства оборони України. URL: https://www.mil.gov.ua/news/2024/03/28/minoboroni-inicziyuvalo-robotu-nad-zakonodavchim-viznachennyam-ponyattya-kibervijna (дата звернення: 11.06.2024).

3 Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України від 10.11.2017 № 45. Стр. 42. С. 403.

Секція 5
АНАЛІТИЧНА РОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ: СТАН, ВИКЛИКИ ТА МАЙБУТНЄ

ЕФЕКТИВНІСТЬ ТА АВТОМАТИЗАЦІЯ: МОЖЛИВОСТІ ШІ В СУЧАСНІЙ OSINT (OPEN SOURCE INTELLIGENCE) АНАЛІТИЦІ

Леонід БАРАШ
доктор філософії у галузі права
судовий експерт ННЦ
«ІСЕ ім. Засл. проф. М.С. Бокаріуса»
Марина ЩЕРБАНЬ
співробітник Служби безпеки України

Використання штучного інтелекту (далі – ШІ) у розвідці з відкритих джерел інформації (далі – ОСІНТ) стає все більш ефективним інструментом для аналітичних служб СБ України, діяльність яких пов'язана зі збором та аналізом інформації. ШІ значно підвищує продуктивність, точність та швидкість обробки великих масивів даних з різноманітних відкритих джерел, таких як онлайн-медіа, соціальні мережі, блоги та форуми. Завдяки автоматизації рутинних завдань, ШІ дозволяє фахівцям зосередитися на більш складних та аналітичних аспектах розвідки, що призводить до більш глибоких і обґрунтованих висновків.

У цій доповіді будуть розглянуті можливості та переваги використання ШІ у ОСІНТ, включаючи збір, обробку, аналіз та візуалізацію даних, а також часова ефективність у порівнянні з традиційними методами.

Почнемо з огляду можливостей ШІ в ОСІНТ, до яких відносяться:

Автоматизація збору даних. Веб-скрапінг: використання ботів для автоматичного збору інформації з веб-сайтів. API-інтеграції: підключення до різних сервісів та платформ для автоматизованого отримання даних.

Аналіз тексту. Натуральна обробка мови (NLP): аналіз текстових даних для виявлення ключових слів, настроїв, тем та трендів. Розпізнавання іменованих сутностей (NER): виділення імен, місць, організацій та інших важливих сутностей у тексті.

Соціальні мережі. Аналіз соціальних мереж: вивчення взаємодій та поведінки користувачів для виявлення впливових осіб, розповсюдження інформації та інших патернів.

Соціально-демографічний аналіз. Аналіз аудиторії: вивчення соціально-демографічного складу аудиторії інфлюєнсерів, включаючи вік, стать, географічне розташування. Поведінковий аналіз: оцінка поведінкових характеристик аудиторії, включаючи рівень залученості, реакції на контент та активність у коментарях.

Аналіз підтримки або критики. Моніторинг реакцій ЗМІ: відстеження публікацій у різних медіа щодо діяльності інфлюєнсерів-націоналістів для визначення, які ЗМІ підтримують або критикують їх діяльність. Тональність статей: використання аналізу тональності для визначення загального настрою статей щодо конкретних інфлюєнсерів, що допомагає зрозуміти позицію кожного ЗМІ.

Порівняння контенту. Виявлення збігів у публікаціях: аналіз текстів для виявлення схожих або тотожних фраз у публікаціях різних ЗМІ або публічних осіб, що може вказувати на ко-

ординовані інформаційні кампанії. Порівняння риторики: аналіз мови та риторики, що використовуються у публікаціях, для виявлення спільних тем та патернів у висвітленні діяльності інфлюєнсерів.

Часовий аналіз. Аналіз трендів: відстеження зміни активності інфлюєнсерів у часі, включаючи піки активності, частоту публікацій та залученість аудиторії. Виявлення патернів: ідентифікація типових часових патернів у публікаціях, таких як частота виходу контенту, що може вказувати на організовані кампанії.

Обробка мультимедіа. Розпізнавання обличь: ідентифікація осіб на фотографіях та відео. Аналіз зображень та відео: виявлення об'єктів, сцен та подій у візуальних даних.

Інтеграція даних. Ф'южн даних: поєднання даних з різних джерел для створення повнішої картини подій або осіб. Геолокація: визначення місцеположення подій або осіб на основі аналізу даних.

Прогнозування. Машинне навчання: використання алгоритмів для прогнозування трендів, подій або поведінки на основі історичних даних.

Автоматизований юридичний аналіз. Аналіз судових документів: ШІ автоматизує аналіз судових рішень, документів та інших матеріалів, виділяючи ключові деталі, що важливі для розслідування або судового розгляду. Це значно скорочує час ручного аналізу та мінімізує ймовірність помилок. Виявлення юридичних ризиків: ШІ допомагає виявляти потенційно ризиковані положення або невідповідності в контрактах та угодах, запобігаючи юридичним проблемам та забезпечуючи відповідність законодавству.

Виявлення правових прецедентів. Ідентифікація релевантних судових рішень: ШІ швидко знаходить прецедентні рішення, що скорочує час на пошук та аналіз судових практик. Аналіз історичних даних: ШІ аналізує історичні судові рішення для виявлення патернів і тенденцій, що корисні для стратегії захисту або обвинувачення.

Юридичні консультації. Віртуальні асистенти: ШІ створює віртуальних асистентів для надання юридичних консультацій у реальному часі, допомагаючи з базовими питаннями та підготовкою до судових слухань. Онлайн-консультації: інструменти ШІ підтримують онлайн-платформи для юридичних консультацій, надаючи відповіді на типові запитання та допомагаючи у вирішенні юридичних проблем дистанційно.

Аналітично-статистичні можливості ШІ у вивченні та аналізі інтернет-видань

Штучний інтелект в ОСІНТ значно підвищує ефективність збору, обробки та аналізу інформації. Автоматизація веб-скрапінгу, аналіз тексту та мультимедіа дозволяє швидко виявляти ключові сутності та тренди. Інтеграція даних і прогнозування створюють повнішу картину подій, роблячи ШІ незамінним інструментом для аналітиків. Аналітики ОСІНТ зазвичай використовують загальний процес аналізу інформації, який включає такі етапи: збір даних, попередня обробка даних, аналіз даних, візуалізація та звітування.

Так, під час здійснення аналітичної діяльності ШІ на будь-якому етапі вже доводить свою ефективність. Для математичного порівняння часу, який потрібен звичайній людині та ШІ для здійснення статистичного аналізу та обробки даних з відкритих джерел, розглянемо декілька основних етапів процесу. Ми оцінюватимемо час, необхідний на кожному етапі, для обробки однакового обсягу даних. Припущення: обсяг даних: 1000 статей (або еквівалентних текстових блоків); кількість слів у кожній статті: приблизно 500 слів; оцінюється час на один цикл (збір, обробка, аналіз, звітування); звичайна людина ефективно може працювати 8 годин на день. Перейдемо до порівняння:

Людина

- Збір: 10,42 днів (час на ручний збір однієї статті: 5 хвилин, з урахуванням пошуку, копіювання, вставки. Загальний час на збір 1000 статей: 5 хв./ст.×1000 ст.=5000 хв. = 83,33 год. ≈ 10,42 днів);
- Обробка: 4,17 днів (час на обробку однієї статті, очищення тексту, видалення зайвих даних: 2 хвилини. Загальний час на обробку 1000 статей: 2 хв./ст. * 1000 ст. = 2000 хв. = 33,33 год. / 8 год./день ≈ 4,17 днів);

– Аналіз: 20,83 днів (час на аналіз однієї статті, виявлення ключових слів, настроїв, трендів: 10 хвилин. Загальний час на аналіз 1000 статей: 10 хв./ст.×1000 ст.=10000 хв. = 166,67 год. / 8 год./день ≈ 20,83 днів);
– Візуалізація: 5 днів (час на підготовку звіту для 1000 статей. 40 год. / 8 год./день = 5 днів).

Разом: 10,42 + 4,17 + 20,83 + 5 = 40,42 днів

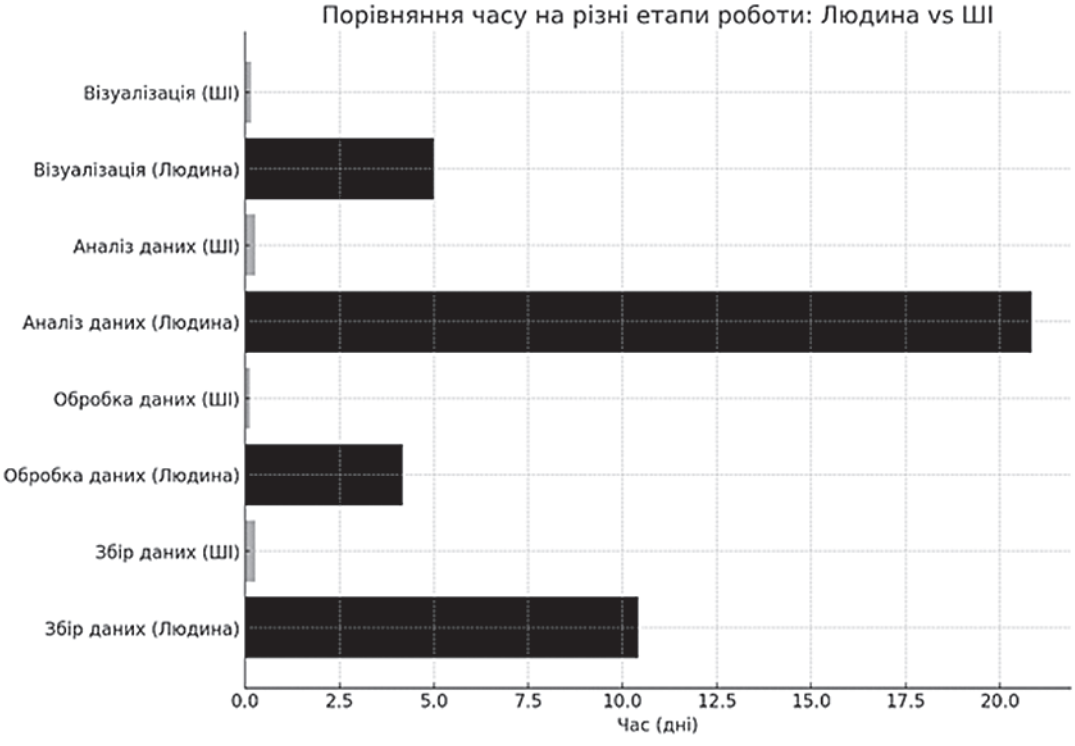
ШІ

– Збір: 16,67 хвилин (час на автоматизований збір однієї статті: 1 секунда, включаючи скрапінг та збереження. Загальний час на збір 1000 статей = 1 сек./ст. × 1000 ст. = 1000 сек. = 16,67 хв.);
– Обробка: 8,33 хвилин (час на автоматизовану обробку однієї статті: 0,5 секунди. Загальний час на обробку 1000 статей: 0,5 сек./ст.×1000 ст.=500 сек. = 8,33 хв.);
– Аналіз: 16,67 хвилин (час на автоматизований аналіз однієї статті: 1 секунда. Загальний час на аналіз 1000 статей: 1 сек./ст.×1000 ст.=1000 сек.= 16,67 хв.);
– Візуалізація: 10 хвилин (час на автоматизовану візуалізацію та підготовку звіту:10 хвилин)

Разом: 16,67 + 8,33 + 16,67 + 10 = 51,67 хв. ≈ 0,86 години

ШІ працює приблизно у 1120 разів швидше, ніж людина (40,42 днів / 0,036 дня ≈ 1120).[1]

Таким чином, використання ШІ для збору, обробки, аналізу та візуалізації даних з відкритих джерел значно скорочує час та ресурси, необхідні для виконання цієї роботи, що робить його надзвичайно ефективним інструментом, однак для використання в аналітичній роботі ШІ потрібні додаткові завдання, які виконує людина, такі як надання правильних промптів, перевірка та валідація результатів ШІ, а також кінцевий огляд звіту.



ШІ може автоматизувати процес збору даних з різних джерел, таких як соціальні мережі, новинні сайти та блоги, що дозволяє обробляти великі обсяги інформації за лічені хвилини, замість днів або навіть тижнів, які потрібні для ручної роботи. Це значно скорочує час, необхідний для виконання рутинних завдань, і дозволяє правоохоронцям зосередитись на стратегічних рішеннях.

[1] (Діаграма, яка порівнює час, необхідний людині та ШІ для виконання різних етапів роботи, включаючи збір даних, обробку даних, аналіз даних та візуалізацію.)

Застосування ШІ також мінімізує людський фактор і пов'язані з ним помилки. Автоматизація рутинних завдань, таких як збір і попередня обробка даних, знижує ймовірність помилок, що можуть виникнути через втому або неуважність. Крім того, ШІ здатен швидко перевіряти та верифікувати зібрану інформацію, виявляючи фейкові новини та дезінформацію, що підвищує загальну достовірність даних. Зазначене, у свою чергу, знижує навантаження на людський ресурс і забезпечує більш ефективне використання часу та енергії співробітників.

Окрім цього, ШІ дозволяє здійснювати глибокий аналіз контенту, виявляти ключові слова, теми, тональність та порівнювати великі обсяги текстів для виявлення збігів і координації між різними джерелами, що особливо корисно для виявлення та аналізу інформаційних кампаній та поведінкових патернів. Моделі машинного навчання також можуть використовуватися для створення прогнозів на основі історичних даних, що допомагає в плануванні та прийнятті обґрунтованих рішень.

В результаті, використання ШІ дозволяє правоохоронним органам значно підвищити свою ефективність, скоротити час на обробку даних і знизити ризики, пов'язані з людським фактором. Це робить ШІ незамінним інструментом для сучасних спецслужб, що прагнуть забезпечити безпеку та правопорядок в умовах швидко змінюваного інформаційного середовища.

Список використаних джерел:

1. Chollet, F. (2017). Deep Learning with Python. Manning Publications. ISBN: 978–1617294433 URL: https://dokumen.pub/python-9785446107704.html. (дата звернення 10.05.2024)

2. Leskovec, J., Rajaraman, A., & Ullman, J. D. (2014). Mining of Massive Datasets. Cambridge University Press. ISBN: 978–1107077232 URL: https://dblp.org/rec/books/cu/LeskovecRU14.html (дата звернення 10.05.2024).

3. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach. Pearson. ISBN: 978–0134610993 URL: https://www.reddit.com/r/Scholar/comments/i1ezt7/book_artificial_intelligence_a_modern_approach/ (дата звернення 10.05.2024).

4. Silver, N. (2012). The Signal and the Noise: Why So Many Predictions Fail – but Some Don't. Penguin Books. ISBN: 978–0143125082 URL: https://www.researchgate.net/publication/374682131_Navigating_Uncertainty_an_Interval_Method_to_Uncover_Export_Dynamics_-_Insights_from_the_Republic_of_Armenia (дата звернення 10.05.2024).

5. Bhardwaj, A., Perez, J., Tiwari, A., & De, A. (2020). «AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems». SN Computer Science. https://link.springer.com/article/10.1007/s42979–022–01043-x (дата звернення 10.05.2024).

БЮРО ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ: НОВИЙ АНАЛІТИЧНИЙ ПІДХІД ДО БОРОТЬБИ З ЕКОНОМІЧНИМИ ЗЛОЧИНАМИ

Олексій БАРБАШОВ
співробітник БЕБ у м. Києві

У воєнний період економічна система України зіткнулася з серйозними проблемами, які вплинули на інвестиційний клімат, зменшення кількості робочих місць та надходжень податків (збрів) до державного бюджету України. Для зменшення цих ризиків і загроз Уряд України приділяє особливу увагу підвищенню можливостей правоохоронних органів, які здійснюють діяльність у сфері економічної безпеки. Основним правоохоронним органом, відповідаль-

ним за запобігання, виявлення та розслідування кримінальних правопорушень, що посягають на функціонування економіки держави є Бюро економічної безпеки України. Бюро економічної безпеки України (далі – БЕБ), згідно частини 1 статті 14 Закону України «Про Бюро економічної безпеки України» (далі – Закон), є юридичною особою публічного права та здійснює свої повноваження через центральний апарат і територіальні управління [1].

Завдання БЕБ – забезпечення економічної безпеки держави шляхом протидії правопорушенням, що посягають на функціонування економіки держави. Його основні цілі – захист публічних фінансів держави, детінізація національної економіки, створення конкурентних умов для бізнесу, інтеграція в європейський економічний простір. Варто зазначити, що успішне виконання місії дозволить зміцнити економічну стійкість та невразливість національної економіки до зовнішніх і внутрішніх загроз [2].

Метою діяльності БЕБ є мінімізація та усунення ризиків у сфері економіки із застосуванням найкращих зразків світової практики з цих питань.

Концепція діяльності БЕБ у минулому році будувалася з урахуванням основних засад, закріплених у Комплексному стратегічному плані реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки, схваленому Указом Президента України від 11 травня 2023 року № 273/2023. Зокрема, впроваджено ідеї організації діяльності БЕБ, що передбачають комплексні зміни всіх аспектів функціонування: від підготовки й добору на службу висококопрофесійних працівників до забезпечення ефективності функціонування системи на основі міжнародних стандартів [3].

Варто зазначити, що власне сама ідея створення БЕБ в своїй основі мала на меті створення саме потужного національного аналітичного центру, який би не просто виявляв економічні правопорушення, вчинені суб'єктами господарської діяльності, а й зміг би прогнозував тенденції до правопорушень та упереджував можливість їх скоєння.

Що стосується мене, то я особисто прихильник саме такої концепції БЕБ – аналітичної роботи на випередження. Здатність БЕБ збирати аналітичні дані про ризики, діяти на основі зібраної інформації та ефективно обмінюватись даними з іншими правоохоронними органами, бізнесом та іноземними партнерами, це все дає нам потужну можливість протистояти загрозам у сфері економічної безпеки та упереджувати виникнення нових економічних ризиків.

Фундаментом стратегії аналітичної роботи в БЕБ є запровадження ризик-орієнтованого підходу. Ризик-орієнтований підхід застосовується в роботі інформаційно-аналітичних підрозділів БЕБ для виконання завдань, визначених Законом України «Про Бюро економічної безпеки України».

Йдеться про здатність БЕБ законно збирати інформацію, аналізувати її для своєчасного розслідування. Відповідний Порядок застосування ризик-орієнтованого підходу в БЕБ визначено Наказом (від 01 лютого 2023 № 36).

Закон України «Про Бюро економічної безпеки» визначає що ризиком є загроза, що ідентифікується в бюджетній, податковій, митній, грошово-кредитній або інвестиційній сфері, вплив якої призводить до тінізації економіки та послаблення економічної безпеки держави [4].

Так співробітниками аналітичного Управління ТУ БЕБ у м. Києві на постійній основі здійснюється підготовка аналітичних матеріалів – аналітичних продуктів у формі: висновка аналітика та аналітичної довідки; інформаційного документа та рекомендацій, які скеровуються до державних органів з метою підвищення ефективності прийняття ними управлінських рішень щодо регулювання відносин у сфері економіки.

Співробітниками аналітичних підрозділів БЕБ вживаються заходи, щодо збирання та аналізу інформації про кримінальні правопорушення, що посягають на функціонування економіки держави, а саме мова йде про виявлення наступних ризиків в сфері економіки, актуальних на сьогоднішній день:

– привласнення та розтрата бюджетних коштів;
– недекларування отримувачами бюджетних коштів (переможцями тендерів) податкових зобов'язань;

– махінації з ПДВ;
– безпідставні заявки на відшкодування ПДВ з бюджету;
– множинні маніпуляції зі звітністю платниками акцизного податку;
– невірне застосування ставок орендної плати за землю;
– ухилення від нарахування та сплати податку на прибуток підприємств;
– неповнота нарахування та сплата у неповному обсязі митних платежів;
– виявляються неодноразові систематичні порушення у сфері місцевих податків, зокрема плати за землю. Так, суб'єкти господарювання використовують земельні ділянки не за цільовим призначенням, використовують занижену нормативно-грошову оцінку земель, занижену ставку орендної плати та не враховують індексацію нормативної грошової оцінки при вирахуванні та сплаті податкових зобов'язань.

Як приклад, СГД, які провадять діяльність у сфері торгівлі (землі під ТРЦ, автосалони та інші торгівельні приміщення) користуються земельними ділянками з функціональним призначенням «для будівництва та обслуговування інших будівель громадської забудови», а не «для будівництва та обслуговування будівель торгівлі», що у свою чергу призводить до заниження їх нормативної грошової оцінки у 3,5 разів та відповідно зменшення сплати податків до бюджету.

Окремо, хочеться наголосити, що у сучасних умовах економічна безпека України безпосередньо залежить від ефективності функціонування митної системи, адже правопорушення в митній сфері призводять до значних економічних втрат, підривають фінансову стабільність держави. Так, за оцінкою експертів, щорічні втрати державного бюджету України від митних правопорушень складають мільярди гривень.

Таким чином фахівці аналітичних підрозділів БЕБ щоденно ідентифікують ризики вчинення підслідних БЕБ правопорушень в митній сфері, а саме:

І. Експорт зерна

При проведенні інформаційно-аналітичної роботи, виявлено, що зацікавлені у вивезенні зерна із митної території України, групи осіб:

– реєструють СГД на підставних осіб та скупляють зерно за готівку;
– у податковій звітності реєструють фіктивні податкові накладні для підтвердження ланцюга постачання зерна;
– укладають контракт про продаж зерна «афілійованим» компаніям за кордоном;
– експортують зерно, у більшості випадків із зазначенням заниженої вартості;
– не повертають в Україну валютну виручку від продажі зерна.

ІІ. Експорт насіння соняшнику

Так, зацікавлені у вивезенні насіння соняшнику із митної території України, групи осіб:

– реєструють СГД на підставних осіб та скупляють соняшник за готівку;
– у податковій звітності реєструють фіктивні податкові накладні про закупівлю соняшнику;
– для підтвердження українського походження соняшнику звертаються до митних органів із заявами про видачу сертифіката походження товару EUR.1, до якої додають фіктивні документи про походження товару;
– експортують соняшник до країн Євросоюзу із використанням так званих преференцій, зменшуючи ставки вивізного мита з 10% до 1,8% від митної вартості.

ІІІ. Експорт металобрухту

Так, зацікавлені у вивезенні металобрухту із митної території України, групи осіб:

– реєструють СГД на підставних осіб та скупляють металобрухт за готівку;
– у податковій звітності реєструють фіктивні податкові накладні про закупівлю металобрухту у СГД, у яких по ланцюгу постачання в ЄРПН його немає;
– на мою думку, дуже актуальною та значущою є проблематика того, що при митному оформлені експорту брухту, відповідно до положень угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної

енергії і їхніми державами-членами, з іншої сторони, СГД користуються преференцією зі сплати вивізного (експортного) мита при поставках до країн Євросоюзу, та ставка вивізного мита при підтвердженні українського походження товару зменшується з 180 євро за 1 тону до 3 євро за 1 тону товару. Ураховуючи, що аналізом податкової звітності встановлюються факти, які можуть свідчити про сумнівність походження металобрухту, що експортується СГД, та відповідно про фіктивність ланцюга постачання від контрагентів-постачальників до експортера, можна зробити висновок, що компанії, надають митним органам фіктивні документи для підтвердження металобрухту українського походження, які не можуть бути законною підставою для зменшення розміру вивізного мита. Суми умовного нарахування та не сплати СГД частки експортного мита при експорті товару позиції 7204 УКТ ЗЕД може становити сотні мільйонів гривень на рік [5].

IV. Імпорт товарів під виглядом благодійної допомоги

До 1 квітня 2024 року пропуск благодійної допомоги здійснювався шляхом подання в пункті пропуску у паперовому вигляді декларації про товари, що заявляються як гуманітарна допомога, із зазначенням кінцевого користувача товарів та гарантійного листа від нього за встановленою формою.

Виходячи з вищезазначеного, мали місце численні зловживання у вигляді ввезення під виглядом благодійної допомоги товарів, які не спрямовувалися за призначенням, а в свою чергу, були реалізовані на внутрішньому ринку без сплати податків.

Підсумовуючи вищезазначене, хочу сказати, що перед Бюро економічної безпеки України стоїть надзвичайно складне, але неймовірно важливе завдання сьогодення, адже створення БЕБ є важливим кроком у зміцнені економічної безпеки держави. Незважаючи на численні виклики, БЕБ має всі шанси стати ефективним органом боротьби з економічними злочинами. Плідна робота бюро сприятиме підвищенню економічної стабільності, зростанню довіри до державних інститутів та створення сприятливих умов для розвитку бізнесу в Україні.

Список використаних джерел:

1. Про Бюро економічної безпеки України: Закон України від 28.01.2021 № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-IX#Text. (дата звернення 19.05.2024)

2. Деякі питання організації діяльності Бюро економічної безпеки України: Постанова Кабінету Міністрів України від 6 жовтня 2021 р. № 1068 URL: https://zakon.rada.gov.ua/laws/show/1068–2021-%D0%BF#n26. (дата звернення 19.05.2024)

3. Звіт про діяльність Бюро економічної безпеки України за 2023 р. URL: https://esbu.gov.ua/storage/app/sites/32/2023%20%D1%80%D1%96%D0%BA/%D0%97%D0%B2%D1%96%D1%82%20%D0%BF%D1%80%D0%BE%20%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D1%96%D 1%81%D1%82%D1%8C%20%D0%91%D0%95%D0%91%20%D0%B7%D0%B0%202023%20%D1%80%D1%96%D0%BA.pdf. (дата звернення 19.05.2024)

4. Про затвердження Порядку застосування ризик-орієнтованого підходу в Бюро економічної безпеки України: Наказ БЕБ від 01.02.2023 № 36, URL: https://zakon.rada.gov.ua/laws/show/z0350–23#Text. (дата звернення 19.05.2024)

5. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Угода, Список, Міжнародний документ від 27.06.2014, URL: https://zakon.rada.gov.ua/laws/show/984_011#Text. (дата звернення 19.05.2024)

ВИКОРИСТАННЯ ЕКСПЕРТНИХ ТЕХНОЛОГІЙ В ІНФОРМАЦІЙНО-АНАЛІТИЧНОМУ ЗАБЕЗПЕЧЕННІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Володимир БОНДАР
кандидат юридичних наук, професор,
співробітник СБУ

Обов'язковою умовою результативного проведення розслідування злочинів проти основ національної безпеки України є належне інформаційно-аналітичне забезпечення.

Останнім часом надзвичайно збільшився потік інформації, що надходить на адресу спеціалізованих підрозділів, які здійснюють протидію злочинам проти основ національної безпеки України, зросла кількість оперативних документів, які потребують негайного прийняття рішення. Гранично зріс обсяг спеціалізованих обліків. Майже жодна з інформаційних систем не є повноцінною аналітичною, адже не може надати повну, вичерпну та цілісну інформаційну картину, котра описує об'єкт або подію. Тому можна стверджувати, що створення кінцевого документа шляхом аналізу, зіставлення та об'єднання проміжних результатів, отриманих з різних інформаційних підсистем є можливим тільки в ручному режимі, унікальних навичок та високої кваліфікації співробітників, оскільки є продуктом суб'єктивного сприйняття, а спроби інтеграції різних інформаційних середовищ, у більшості випадків, приречені на невдачу. Основними перешкодами можуть стати відмінності форматів зберігання даних або самих даних, у яких зберігається інформація.

У цих умовах першочергового значення набуває активізація та удосконалення політики в сфері діяльності органів правопорядку щодо протидії кримінально-протиправній діяльності у сфері національної безпеки України, що має на меті створення такої організаційної та інформаційно-технологічної інфраструктури, та умов її функціонування, які б забезпечували максимально ефективну інформаційно-аналітичну підтримку боротьби зі злочинністю та її профілактики. Результатом практичної реалізації такої роботи повинно стати формування єдиного інформаційно-правового середовища органів правопорядку щодо протидії злочинності, створення ефективної системи інформаційно-аналітичного забезпечення органів правопорядку та забезпечення її постійного розвитку на базі сучасних досягнень науки і техніки.

На думку автора, комплекс інформаційно-аналітичного забезпечення розслідування злочинів розглядуваної категорії повинен забезпечувати таке:

– вибір системи ключових об'єктів аналізу з метою формування складної багаторівневої характеристики тієї чи іншої події, яка враховує всі взаємозв'язки, що виникають у процесі її розвитку;
– погодження стратегічних й тактичних задач розслідування з прийнятою системою об'єктів аналізу (час, місце, спосіб, обстановку події, матеріальний слід-відображення тощо). Серед типових тактичних задач можна назвати встановлення події злочину; встановлення особи, яка вчинила злочин за залишеними нею слідами: IP-адресою, MAC-адресою, адресою електронної пошти, ідентифікатором соціальної мережі, номером банківської картки, номером телефону, інформацією про з'єднання абонента, проведенням транзакції тощо; встановлення шкоди та забезпечення її відшкодування; встановлення обставин вчинення злочину; доведення винності особи у вчиненні злочину тощо. Метою інформаційного аналізу повинен стати збір максимально повного набору ідентифікаційних даних, які мають відношення до такої особи. У якості таких даних можуть виступати а) номери мобільних телефонів, номери IMEI та IMSI; б) MAC-адреси персональних комп'ютерів, планшетів, смартфонів; г) аккаунти та паролі в соціальних

мережах; ґ) логіни та паролі доступу в Інтернет (у тому числі WiFi тощо), інформація про використаних особою предметах з RFID-позначками, ґаджетах, які мають вихід до Інтернету, інші цифрові мережі передачі даних (пульсометри, крокоміри тощо); д) аккаунти та паролі в електронній пошті, системах комп'ютерної комунікації, мережевих комп'ютерних іграх; е) номери та реквізити банківських карток, електронних платіжних систем, якими послугувалася людина, що безвісти зникла, тощо; є) проїзні документи, які використовувалися особою останнім часом; ж) позначення місць розташування (геотеги) у створених останнім часом файлах фотографій (у телефонах, планшетах, фотоапаратах, комп'ютерах), маршрутах в GPS-навігаторах;

– перетворення обраних об'єктів у форму, необхідну для їх обробки та аналізу комплексом інформаційно-аналітичного забезпечення криміналістичної діяльності;
– складання схем мережі зв'язків на кожного фігуранта;
– аналіз зв'язків об'єктів обліку – елементів інформаційної системи, отримання знань із використанням методик аналізу;
– аналітичну перевірку (прогнозування) наслідків запланованих процесуальних рішень під час досудового розслідування на предмет їх відповідності системі цільових критеріїв;
– підготовку аналітичних документів.

За рахунок застосування різноманітних методів аналітичної обробки можливо досягнути таких результатів:

– здійснити позиціонування абонентів мобільного зв'язку на місцевості в конкретні моменти часу;
– визначити коло потенційних свідків подій, які відбувалися в певні моменти часу;
– виявити коло спілкування особи (друзі, соціальні мережі).

Іншими словами, можливості використання інформаційних технологій та аналітичних методів обробки великих обсягів різнорідної цифрової інформації під час досудового розслідування злочинів проти основ національної безпеки, потенційно фактично необмежені. Сьогодні не існує перешкод для розробки конкретних алгоритмів розв'язання криміналістичних задач на базі аналізу великих обсягів інформації.

Відмінною особливістю задач інформаційно-аналітичного забезпечення відповідної криміналістичної діяльності, на думку автора, є його націленість на кінцевий результат – на підкріплене аналізом процесуальне рішення, у той час як завданням інформаційного забезпечення є постачання інформації суб'єкту розслідування.

Під час формування та впровадження інформаційно-аналітичного забезпечення криміналістичної діяльності аналітик постійно оперує показниками, адже найбільш ефективним способом опису об'єкта аналізу є його подання шляхом показників. Аналітичне забезпечення, тобто методики та методи аналізу, направлені на вимірювання показників, аналіз динаміки та прогнозування значень показників, а також контроль над досягненням їх цільових значень. Таким чином, одиницею інформаційно-аналітичного забезпечення криміналістичної діяльності є показник.

Показники, отримані шляхом обробки даних у контексті цілей та задач, наприклад, досудового розслідування серійних убивств, є важливою частиною інформації.

Дослідження обставин учинення злочинів проти основ національної безпеки України дозволяє виокремити такі основні види інформації, що піддається логіко-структурному аналізу, яка містить ознаки їх вчинення одними й тими ж особами та сприяє віднесенню злочинів.

1. Судово-медична – причина та час настання смерті; характер та локалізація тілесних ушкоджень на трупах потерпілих; ознаки завдання тілесних ушкоджень після оголення тіла жертви; розсічення, повна або часткова ампутація зовнішніх та внутрішніх статевих органів; використання однотипних знарядь убивства; ознаки знущання над трупом у вигляді посмертних тілесних ушкоджень; наявність на трупі нетипових пошкоджень (ампутація пальця, носа; розсічення серця; перерізання шиї та інші).

2. Медико-криміналістична – сліди зубів на тілах потерпілих, які утворилися при укусах; характерні сліди знарядь убивств на тілах потерпілих та знарядь розчленування на кістках та хрящах трупів та їх фрагментів.

3. Трасологічна – сліди рук на предметах обстановки та на знаряддях злочинів; сліди взуття на місцях подій; сліди зубів на недопалках; сліди транспортних засобів навколо місць виявлення трупів; сліди рублячих та ріжучих знарядь на гілках, якими маскуються трупи. У випадках, коли злочинці зв'язують руки або заклеюють рота людям, які піддалися нападам та катуванням, липкою стрічкою («скотчем») або ізоляційною стрічкою, сліди рук нападників можуть залишитись на такій стрічці; сліди-нашарування мікрочасток у вигляді волокон, які відрізняються від інших у складі тканини одягу потерпілих та мають однакове походження з мікрочастками, виявленими за іншими епізодами вбивств; мікрочастки на деталях обстановки місця події; у змісті піднігтьових лож трупів потерпілих.

4. Балістична – стріляні з одного й того ж екземпляра нарізної вогнепальної зброї: а) кулі, вилучені з тіл потерпілих, а також виявлені на місцях подій за різними епізодами вбивств; б) стріляні гільзи; в) патрони зі слідами перебування в казенній частині одного й того ж екземпляра зброї, знайдені на різних місцях злочинів; г) подібність складу гомогенного металу для куль та ознаки використання однієї й тієї ж зброї для виготовлення пижів і прокладок до патронів для гладкоствольної зброї.

5. Біологічна – кров на одязі потерпілих та в змісті піднігтьових лож їхніх рук; слина на недопалках сигарет, випалених злочинцями (вони можуть знаходитися як на місці вбивства, так і на тому містині, звідки злочинець виглядав жертву); потожирова речовина на головних уборах, рукавичках, предметах одягу злочинця, на знаряддях убивств; носовий слиз на носових хустинках, які не належать потерпілим; сперма на предметах одягу, білизни та на тілах потерпілих, на тампонах з мазками з їхніх трупів; волосся на місцях подій, на тілі, у пальцях рук трупів, на їхньому одязі; частини епітеліальної тканини в піднігтьовому змісті потерпілих; кров у слідах, які утворилися в результаті травмування злочинця на місцях подій.

6. Запахова – проби повітря з місць подій; на знаряддях убивств та інших об'єктах, які не належать потерпілим; на одязі потерпілих, який контактував із одягом, руками, тілом злочинця; у слідах крові, виділень та у волоссі суб'єкта злочину.

7. Технічна (конструкторсько-технологічна) – конструктивні особливості будови та технології виготовлення знарядь злочинів (наприклад, атипової вогнепальної зброї шляхом розсвердлювання стволів газових пістолетів та виготовлення вкладок під них, що забезпечують стрільбу штатними патронами); пристроїв до вогнепальної зброї (саморобних глушників та пістолетів та пістолетів-кулеметів); сліди обладнання та інструментів, які використовувалися для виготовлення зазначених об'єктів.

8. Інша криміналістична – розташування в укритих місцях, які дозволяють попередньо спостерігати за жертвою, а потім непомітно та раптово нападати на неї; знаходження місць подій поблизу зупинок транспорту; характерні ознаки місць приховання трупів жертв, які дають підставу передбачати добре знання злочинців цієї місцевості та інші; наявність групи суб'єктивних портретів, подібних один одному; обличчя ймовірних злочинців, складених художниками-криміналістами методом суб'єктивного рисованого портрету або створення «фотороботу» за показаннями потерпілих, які залишилися в живих, або свідків; збіг часу вбивств; учинення злочинів в одні й ті самі дні тижня тощо.

Аналітична обробка інформаційних масивів повинна створювати умови для встановлення осіб, підозрюваних у скоєнні кримінальних правопорушень та інших обставин, які мають значення для вирішення завдань розслідування. Роль інформаційно-аналітичного забезпечення має зводитись до якісно-змістовному перетворенню інформації про подію злочину з метою отримання результату у взаємодії елементів системи «аналітика – нове знання – процесуальне рішення». Інтеграція обліків та колекцій буде сприяти формуванню єдиного інформаційного простору та забезпеченню безперервного процесу обробки інформації на основі ресурсів органів внутрішніх справ та Національної поліції. Таким чином, система інформаційного за-

безпечення повинна являти собою відкритий інформаційний контур, який охоплює всі сфери діяльності людини. При цьому необхідним є перехід з однієї сфери в іншу за сукупністю функціональних та логічних зв'язків.

Виконання цих завдань створить умови для вирішення важливих завдань:

– забезпечувати збір максимально повної інформації про об'єкти інтересу з формуванням «електронного досьє» на потенційних суб'єктів злочинів, виявленням та візуалізацією неявних зв'язків з іншими об'єктами та подіями кримінального характеру;
– фіксувати соціальну активність розроблюваних осіб, виникнення та зміну їх мережевих зв'язків, аналізувати ступінь інтересу до них;
– покращувати планування слідчих (розшукових) дій та негласних (розшукових) дій за рахунок урахування складної сукупності численних факторів, які впливають на розвиток конкретної слідчої ситуації;
– формувати комплекс методичних рекомендацій на основі аналізу постійно поповнюваного масиву всіх слідчих ситуацій та варіантів їх розвитку.

Таким чином, використання експертних технологій в інформаційно-аналітичному забезпеченні розслідування проти основ національної безпеки повинен забезпечувати:

– вибір системи ключових об'єктів аналізу;
– погодження стратегічних й тактичних задач розслідування з прийнятою системою об'єктів аналізу (час, місце, спосіб, обстановку події, слід-відображення тощо);
– перетворення обраних об'єктів у форму, необхідну для їх обробки та аналізу комплексом інформаційно-аналітичного забезпечення криміналістичної діяльності;
– складання схем мережі зв'язків на кожного фігуранта;
– аналіз зв'язків об'єктів обліку – елементів інформаційної системи, отримання знань із використанням методик аналізу;
– аналітичну перевірку (прогнозування) наслідків запланованих процесуальних рішень під час досудового розслідування на предмет їх відповідності системі цільових критеріїв;
– підготовку аналітичних документів.

Список використаних джерел:

1. Бахуринська О.О. Перспективні напрями протидії організованій злочинності в Україні. Право і суспільство. 2018. № 6. С. 182–188.

2. Бірюков В.В. Інформаційно-довідкове забезпечення кримінальних проваджень: підручник / В.В. Бірюков, В.Г. Хахановський, В.С. Бондар; за заг. ред. В.В. Бірюкова. Київ: Центр учбової літератури, 2014. 288 с.

3. Користін О.Є., Свиридюк Н.П. Національні реалії впровадження методології Європолу «SOCTA». Південноукраїнський правничий часопис. 2022. № 1–2. С. 109–114.

4. Мовчан А.В., Созанський Т.І. Характерні ознаки сучасної організованої злочинності за результатами опитування Socta. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. № 1. 2023. С. 49–56.

5. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.

СПОСІБ РОЗРАХУНКУ СПРОМОЖНОСТЕЙ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

Юрій МІХЄЄВ
кандидат технічних наук, старший дослідник,
доцент кафедри інформаційної боротьби
Національного університету оборони України

На сьогоднішній день росія не припиняє своїх загарбницьких намірів по відношенню до України. Головним наміром таких діє є захоплення українських територій за рахунок використання силових методів (власних збройних сил (ЗС) та керування незаконними збройними формуваннями), ведення інформаційно-психологічних операцій та запровадження агресивної політики по відношенню інших держав [1]. В таких умовах протистояння російській агресії вимагає від керівництва ЗС України (органів військового управління, командирів підрозділів) прийняття ефективних рішень під час виконання планування та проведення відповідних операцій (бойових дій).

Особливість роботи органу військового управління при плануванні та веденні операції (бойових дій) пов'язана з безперервним процесом збору, накопичування, збереження та обробки великих обсягів інформації і супроводжується виконанням різноманітних розрахунків кількісних показників і характеристик. Цей процес спрямований на всебічне забезпечення підготовки та прийняття рішення та надає командирам можливість об'єктивно розглянути різні варіанти бойових дій і обґрунтовано обрати найбільш ефективне рішення.

Одним з можливих шляхів підвищення ефективності планування операції (бою) можливо за рахунок вчасного отримання, оброблення та підготовки необхідних даних для подальшого, зниження часу проведення оперативно-тактичних розрахунків, розроблення та оцінювання варіантів рішень. Тому сьогодні актуальним постає питання удосконалення системи інформаційно-аналітичного забезпечення (ІАЗ) ЗС України з урахуванням набутого досвіду під час виконання завдань відповідними підрозділами протягом російсько-української війни.

Завдання з удосконалення системи ІАЗ підрозділів ЗС України потребує у свою чергу розгляду ряду питань щодо:

- обґрунтування переліку спроможностей суб'єктів інформаційно-аналітичної діяльності в ЗС України;
- розроблення способу оцінювання спроможностей інформаційно-аналітичних підрозділів ЗС України, для подальшого аналізу ефективності кожного елементу системи ІАЗ, що може бути удосконалений, та виключення ймовірних вразливостей у процесі функціонуванні системи ІАЗ.
- У доповіді подано спосіб оцінювання спроможностей інформаційно-аналітичних підрозділів ЗС України. Запропоновано показники та критерії оцінювання спроможностей інформаційно-аналітичних підрозділів Збройних Сил України, які враховують особливості виконання ними завдань. Розроблені показники дозволять кількісно оцінити спроможності інформаційно-аналітичного підрозділу відповідно напрямів його роботи, а саме:
- спроможність інформаційно-аналітичного підрозділу зі збору, отримання, доведення інформації до споживачів. Здатність здійснювати постійний моніторинг та своєчасно отримувати якісні інформаційно-аналітичні матеріали.
- спроможність інформаційно-аналітичного підрозділу з проведення аналітичної роботи (обробка, аналіз, перевірка достовірності та актуальності зібраних інформаційно-аналітичних матеріалів). Здатність здійснювати змістовний та якісний аналіз зібраних ін-

формаційно-аналітичних матеріалів та перевіряти зібрані матеріали на достовірність, актуальність, повноту, корисність.

– спроможність інформаційно-аналітичного підрозділу підготовки звітно-інформаційних документів. Здатність формувати звітні матеріали у відповідності до вимог поставленого завдання, виконуваної задачі.

Для розроблення показників та критеріїв оцінювання спроможностей інформаційно-аналітичних підрозділів пропонується використати відомості, зазначені у Єдиному переліку (каталозі) спроможностей Міністерства оборони України, Збройних Сил України та інших складових сил оборони [2].

Використання такого підходу дозволить за участю експертів визначити: кількісну та якісну потребу в технічних та програмних засобах інформаційно-аналітичних підрозділів ЗС України для їх оснащення; оцінити важливість підрозділів, повноту виконання ним функцій та визначити пріоритетні напрями розвитку та набуття ними спроможностей.

Список використаних джерел

1. Левченко О.В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування: монографія / О.В. Левченко.– Житомир: Видавець ПП «Євро-Волинь», 2021.– 172 с.

2. Уточнений Єдиний перелік (Каталог) спроможностей Міністерства оборони України, Збройних Сил України та інших складових сил оборони. МО, наказ «Про затвердження Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони» від 22.12.2020 № 484.

ЗАРУБІЖНИЙ ДОСВІД СПІВРОБІТНИЦТВА СПЕЦСЛУЖБ У СФЕРІ АНАЛІТИЧНОЇ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ

Володимир ПАЛИВОДА
завідувач відділу державної та громадської безпеки
центру безпекових досліджень
Національного інституту стратегічних досліджень
при Президентові України

Влітку 2022 року розвідувальна служба Ізраїлю «Моссад» запустила спеціальну навчальну програму для співробітників європейських спецслужб із ефективного використання потенціалу інструментів розвідки на основі відкритих джерел інформації (далі – OSINT) з метою поліпшення можливостей щодо збору розвідданих та вербувальної діяльності.

За даними зарубіжних експертів, спецслужби Бельгії, Італії та Іспанії протягом кількох років реалізують цю навчальну програму шляхом організації інтенсивних курсів для дуже обмеженого кола осіб, почергово, у столицях згаданих країн. Координацією програми безпосередньо займається «Моссад».

Цей міждисциплінарний обмін методами та практичним досвідом був розроблений колишнім директором «Моссад» Йосі Коеном[1] і підтриманий його наступником Давидом Барнеа. Обидва керівники ізраїльської розвідки, виступаючи перед учасниками курсів, стверджували, що до 80% аналітичної роботи засновано на відкритих джерелах інформації. Водночас вони наголошували, що такі джерела можуть використовуватися тільки в країнах, де існує певна свобода висловлення поглядів.

[1] Очолював «Моссад» у 2016-2021 рр.

Коментуючи цю ситуацію, зарубіжні експерти зазначають, що необхідно мати на увазі наявність в OSINT двох компонентів. З одного боку, це дійсно відкриті джерела, на кшталт загальновідомих заяв, податкових документів та звернень до різних інстанцій, а також контент соціальних мереж. На їхній основі реально отримати дані про фінансове та майнове становище тієї чи іншої особи, її контакти та хобі. У деяких випадках можна зробити висновок і про її політичні симпатії.

З іншого боку, це – електронна пошта, SMS, закриті фінансові та установчі документи, листування у месенджерах, доступ до яких можна отримати лише внаслідок хакерського злому чи домовленості з користувачем того чи іншого месенджера. Хоча, в експертному середовищі вважають, що АНБ США «читає» практично усі західні месенджери. У країнах ЄС з цим складніше через відповідне законодавство, але, як недавно стало відомо, у цьому випадку використовуються ізраїльські шпигунські програми типу «Pegasus».

У рамках курсів для європейських колег відпрацьовується перший компонент. Інструктори «Моссад» пояснюють, як краще поєднувати OSINT із традиційною розвідувальною діяльністю (яка неминуче буває фрагментованою та потенційно упередженою), щоб покращити аналітичні можливості спецслужб.

Ще один момент, якому інструктори «Моссад» приділяють велику увагу, це – критичний підхід до інтерпретації джерел. У кожній спецслужбі є підрозділ, завдання якого ставити під сумнів усі аналітичні матеріали. Така система була розроблена для виявлення критично важливих моментів кожної інтерпретації оперативної обстановки, залишаючи останнє слово за особами, що приймають управлінські рішення.

Дані відкритих джерел використовуються й у вербувальній розробці того чи іншого кандидата, але за допомогою OSINT практично нереально віднайти серйозне джерело інформації. Для цього необхідне первинне агентурне наведення на об'єкта.

Оскільки в Ізраїлі існує певний «розподіл праці» між різними структурами кібершпигунства, другий компонент OSINT виведено за межі офіційних тренінгів. Підвищенням професійного рівня співробітників європейських спецслужб у цій сфері займається одна із провідних ізраїльських компаній «XM Cyber», очолювана колишнім директором «Моссад» Таміром Пардо[1], і яка тісно співпрацює з головною розвідслужбою своєї країни. Власне, тренінги полягають у передачі хакерам, котрі працюють на замовлення спецслужб, потрібних шпигунських програм. У 2021 році ця компанія отримала акредитацію Національного агентства безпеки інформаційних систем Франції і розпочала активне проникнення на європейський ринок.

Ще однією компанією, яку залучали до тренінгів по лінії другого компонента OSINT, була фірма «Labyrinth», заснована колишніми офіцерами ізраїльської військової розвідки Гідеоном Харарі та Яхелем Арноном і консультована згаданим вище Таміром Пардо.

Список використаних джерел

1. Mossad trains European intel agents in open-source spy tools analysis. URL: https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra (дата звернення 04.06.2024).

2. Pegasus spyware called into question by PACE. URL: https://www.coe.int/en/web/freedom-expression/-/pegasus-spyware-called-into-question-by-pace (дата звернення 04.06.2024).

3. Former Israeli spy chief and team of elite hackers form cybersecurity firm. URL: https://www.reuters.com/article/us-israel-cyber-mossad/former-israeli-spy-chief-and-team-of-elite-hackers-form-cybersecurity-firm-idUSKBN1GW1HA/ (дата звернення 04.06.2024).

4. Labyrinth Ltd. Defense & Space. URL: https://il.linkedin.com/company/labyrinth-ltd (дата звернення 04.06.2024).

[1] Очолював «Моссад» у 2011-2016 рр. Після виходу у відставку займається бізнесом. Заснував і очолив компанію «XM Cyber», яка надає платформу для навчання протидії кібератакам (у листопаді 2021 р. компанію за 700 млн доларів придбав німецький концерн «Schwarz Group»). Крім того, заснував та очолив інвестиційну компанію «Other Sources Energy Group» (OSEG), а також створений спільно з гонконгською енергетичною корпорацією «CLP Group» інвестиційний фонд CLP-OSEG.

ДО ПИТАННЯ АНАЛІТИКИ BIG DATA В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

Максим ПАЛЬЧИК
кандидат юридичних наук,
співробітник СБУ

На сьогодні цифровізація проникає в усі сфери суспільного життя, а дані стають ключовою рушійною силою розвитку економіки та суспільства. Вміле та своєчасне використання даних різного роду формує безперечну конкурентну перевагу та в довгостроковій перспективі призводить до розвитку інновацій та технологій. Не є виключенням актуальність застосування великих даних (Big Data) у секторі безпеки та оборони, особливо в умовах триваючої збройної агресії рф проти України.

Big Data – це масиви структурованих і неструктурованих даних великого обсягу, що створені в автоматичному режимі з великої кількості різноманітних джерел, а також методи та способи їх обробки. Великі дані можуть бути згенеровані різноманітними пристроями, зокрема датчиками та сенсорами, що збирають кліматичну, аудіовізуальну інформацію тощо. Джерелами Big Data можуть бути супутникові зображення, цифрові фотографії та відео, записи про транзакції покупок, дані соціальних мереж, сигнали GPS тощо. Big Data охоплює багато секторів, від охорони здоров'я до транспорту, енергетики та оборони.

Тривалий час великі дані не мали великої цінності, оскільки для вивчення інформації потрібні були великі обчислювальні потужності, значна кількість часу та фінансових ресурсів. Водночас зі створенням концепції обчислення MapReduse та появою фреймворку Hadoop використання Big Data зазнало неабиякого розвитку.

Для розуміння обсягів обробки даних за допомогою автоматизованих систем варто зазначити, що станом на травень 2024 року у світі щодня створюється 328,77 мільйонів терабайтів даних, пошукова система Google обробляє близько 8,5 мільярдів пошукових запитів, а користувачі WhatsApp обмінюються до 65 мільярдів повідомлень на день, 80-90% даних, які генеруються на сьогодні, є неструктурованими [1]. Мережа середнього розміру з 20 000 пристроїв (ноутбуків, смартфонів і серверів) передаватиме понад 50 ТБ даних за 24 години. Це означає, що потрібно аналізувати понад 5 Гбіт щосекунди, щоб мати змогу виявити зловмисне програмне забезпечення, потенційні загрози та кібератаки [2].

Використання Big Data тісно пов'язано з розвитком технологій штучного інтелекту, які потребують великих обсягів даних для ефективного навчання нейронних мереж. Ба більше, технології штучного інтелекту усе частіше використовуються для обробки та аналізу великих обсягів даних, що дозволяє автоматизувати ці процеси, заощадити час і ресурси, необхідні для прийняття рішень на основі Big Data.

Робота з великими обсягами даних у режимі реального часу є складним завданням, розв'язати яке можливо за допомогою ефективних механізмів аналізу великих обсягів даних, які можуть використовуватись для створення наукових моделей даних, здатних виявляти негативні системні тренди та загрози, зводячи до мінімуму негативні наслідки від їх реалізації.

В умовах повномасштабного вторгнення рф, Big Data можуть бути як об'єктом зацікавленості ворога, так і ефективним інструментом отримання якісної переваги над ним.

Розглядаючи Big Data як об'єкт зацікавленості ворога, варто наголосити, що від початку збройної агресії суттєво зросла кількість кібератак на інформаційні ресурси України, направлених, у тому числі, на порушення цілісності даних. Найбільше атакують урядові організації, місцеві органи влади та сектор безпеки та оборони, комерційні організації, енергетичний сектор, телекомунікації та багато інших установ.

Рішення на основі Big Data можуть бути також дієвим механізмом у боротьбі з ворогом. У цьому контексті варто зауважити, що ідея збору та аналізу Big Data з численних пристроїв, датчиків та сенсорів, їх обробки за допомогою алгоритмів машинного навчання з використан-

ням значних обчислювальних потужностей, з метою отримання якісної переваги над ворогом, усе частіше знаходить свою підтримку серед військово-політичного керівництва провідних держав світу, які дедалі більше посилюють розробку та впровадження систем, що працюють на основі AI у секторі безпеки та оборони. Суттєво зростає фінансування вказаних проєктів, а також правове забезпечення їх використання.

Так, в бюджетах оборонних відомств окремих країн усе більше коштів передбачається на витрати з дослідження, розробки, тестування та оцінки штучного інтелекту, зокрема в бюджеті Міністерства оборони США на 2024 рік передбачено 1,8 млрд дол. на вказані потреби, у той час як у 2022 році було закладено близько 874 млн дол. [3].

Також приділяється увага визначенню та унормуванню стратегічних напрямів та концептуальних засад обробки Big Data та використання AI в оборонній сфері. Зокрема, у листопаді 2023 року Міністерство оборони США оприлюднило свою Стратегію щодо даних, аналітики та впровадження AI, що направлена, серед іншого, на прискорення впровадження новітніх даних, аналітики та технологій штучного інтелекту задля забезпечення військових керівників різних рівнів необхідними даними для прийняття швидких та ефективних рішень на полі бою [4].

Тренди використання та правового забезпечення Big Data та AI у секторі безпеки та оборони є актуальними і для України. Зокрема, у межах удосконалення інституційних механізмів аналізу та управління ризиками у сфері національної безпеки і оборони України, Апаратом РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему Головного ситуаційного центру країни «СОТА» (ІАС «СОТА»). Вказана система працює з Big Data, забезпечує зберігання, поєднання та аналіз даних з різних джерел задля підвищення достовірності, ефективного моніторингу стану національної безпеки по понад 20 напрямах, з метою ефективної координації діяльності державних органів. Програмні аналітичні модулі ІАС «СОТА» дозволяють забезпечити неупереджений об'єктивний контент-аналіз та синхронізацію значних обсягів даних [5].

Також, у межах розбудови національної системи правового регулювання штучного інтелекту, у грудні 2020 року було схвалено Концепцію розвитку штучного інтелекту в Україні [6]. Серед завдань, направлених на виконання мети Концепції у сфері кібербезпеки, що безпосередньо пов'язані з аналізом даних у сфері кібербезпеки визначено розроблення інноваційних систем кібербезпеки, які широко застосовують технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання. До того ж констатовано, що моніторинг соціальних мереж та інтернет-ресурсів електронних медіа з використанням технологій штучного інтелекту дає можливість виявляти системні тренди і проблематику, діяти на випередження, аналізувати цільову аудиторію.

Документом також передбачено, що для досягнення мети Концепції у сфері оборони слід забезпечити використання технологій штучного інтелекту у системах: командування та управління; озброєння та військової техніки; збору та аналізу інформації під час ведення бойових дій; аналізу/розвідки, підтримки проведення розвідувальних заходів, обробки картографічної інформації; імітаційного та когнітивного моделювання бойової обстановки; когнітивного аналізу спроможностей військових підрозділів, протидії кіберзагрозам у сфері оборони.

Підсумовуючи викладене можемо констатувати, що аналітика Big Data, є складним процесом, у якому досліджуються різноманітні набори даних, з метою виявлення невідомих та прихованих закономірностей, трендів, загроз тощо. В умовах збройної агресії рф проти України саме аналітика Big Data має стати невід'ємною складовою систем підтримки прийняття рішень при забезпеченні інформаційної безпеки, кібербезпеки, та оборони нашої держави.

Список використаних джерел:

1. Aditya Rayaprolu. 25+ Impressive Big Data Statistics for 2024. TechJury. Jan 03, 2024. URL: https://techjury.net/blog/big-data-statistics. (дата звернення 21.06.2024)

2. David Lopes Pegna. Big data sends cybersecurity back to the future. Computerworld. Mar 12, 2015. URL: https://www.computerworld.com/article/1624024/the-future-of-cybersecurity-big-data-and-data-science.html. (дата звернення 21.06.2024)

3. How AI is changing warfare. The Economist. Jun 20th 2024. URL: https://www.economist.com/briefing/2024/06/20/how-ai-is-changing-warfare. (дата звернення 21.06.2024)

4. Deputy Secretary of Defense Kathleen Hicks Announces Publication of Data, Analytics and AI Adoption Strategy. U.S. Department of Defense. Nov 2, 2023. URL: https://www.defense.gov/News/Releases/Release/Article/3577857/deputy-secretary-of-defense-kathleen-hicks-announces-publication-of-data-analyt/. (дата звернення 21.06.2024)

5. В Апараті РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему «СОТА». Рада національної безпеки і оборони України. 22 Вересня 2021. URL: https://www.rnbo.gov.ua/ua/Diialnist/5011.html. (дата звернення 21.06.2024)

6. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text. (дата звернення 21.06.2024)

РОЛЬ АНАЛІТИЧНОЇ РОЗВІДКИ У ПОСИЛЕННІ СПРОМОЖНОСТЕЙ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Дарія ПРОКОФ'ЄВА-ЯНЧИЛЕНКО
доктор юридичних наук, старший дослідник,
заслужений юрист України
Керівник Міжвідомчого науково-дослідного
центру з проблем боротьби з організованою
злочинністю при РНБО України

Відповідно до статті 4 Закону України «Про розвідку» [1], Служба безпеки України є суб'єктом розвідувального співтовариства. При цьому оперативні підрозділи Центрального управління Служби безпеки України, що здійснюють контррозвідувальну діяльність, можуть проводити розвідувальні заходи з метою отримання інформації в інтересах контррозвідки.

Аналітична розвідка – напрямок розвідувальної діяльності (поряд з агентурною, технічною, військовою розвідкою тощо), тобто, система розвідувальних заходів, яка передбачає цілеспрямоване збирання, систематизацію та аналітичну обробку відомостей з метою отримання нових знань про факти, процеси та суб'єктів, які становлять оперативний інтерес.

Аналітична розвідка здійснюється на оперативному та стратегічному рівнях. Оперативна аналітична розвідка досліджує короткочасні феномени для забезпечення відповідної здійснення невідкладної діяльності. Стратегічна аналітична розвідка спрямована на досягнення довготривалих цілей, визначення пріоритетів та загального спрямування діяльності щодо забезпечення національної (державної) безпеки, прогнозування неочевидних та відтермінованих подій, реагування на які потребує реалізації довгострокових, масштабних заходів.

Предметом аналітичної розвідки переважно є відкриті дані, в тому числі й ті, яка не є загальнодоступними (в сучасних умовах це більше 90% даних). В ході аналітичної розвідки можуть використовуватись також дані, зокрема, з обмеженим доступом, здобуті в ході агентурної, технічної, військової розвідки тощо.

Аналітична розвідка може вестися за допомогою гласних, напівгласних і негласних методів, найбільш популярними серед яких є: дослідження офіційної статистики, відомостей з держаних реєстрів, вивчення публікацій в ЗМІ, наукових та аналітичних професійних виданнях; моніторинг глобальної інформаційної мережі Інтернет та месенджерів; методи соціальної інженерії, OSINT тощо.

Зокрема, OSINT (Open Source INTelligence) – це технологія пошуку, акумулювання та аналізу даних, зібраних з відкритих джерел (статистичні дані, сайти оголошень, торгові майданчики, реклама, прес-релізи, блоги, групи та форуми за інтересами, аналітичні огляди, наукові пу-

блікації, патенти, державні реєстри, банківські онлайн-системи, соціальні мережі, опитування тощо), в тому числі й тих, що не є загальнодоступними (зокрема, ресурси з платним доступом, офіційною авторизацією тощо). Відповідні дані можуть розміщуватись у різних формах: статті, пости на форумах, новинних месенджерах, відео- та аудіофайли, документи, зображення тощо, а також на ресурсах, спеціально створених в цілях аналітичної розвідки, зокрема, гейміфікованих застосунках, сайтах для дослідження громадської думки тощо.

На відміну від кіберрозвідки як напрямку технічної розвідки, аналітична розвідка з використанням ресурсів інформаційних систем та мереж не передбачає несанкціонованого доступу до інформації, що циркулює в таких системах та мережах, а також використання таких засобів, як комп'ютерні віруси, «троянські коні», логічні бомби тощо.

Основними методами роботи з інформацією при здійсненні аналітичної розвідки є так звані кількісні (статистичні, фінансові, математичні моделювання) та якісні («метод п'яти сил», SWOT-аналіз, мережі зв'язків, контент-аналіз, аналіз візуальних спостережень, експертні («віч-на-віч», метод комісій, «судового процесу», «мозкова атака»), «сценарний аналіз», метод Делфі, «мудрість натовпу», форсайт-дослідження тощо) методи.

Результатом обробки даних, здобутих в ході аналітичної розвідки, є розвідувальна інформація – сукупність даних, що були відібрані, оброблені і проаналізовані, яка характеризується кількісними (повнота, достатність, обсяг), якісними (актуальність, адекватність, об'єктивність, корисність, доступність, своєчасність, точність, можливість перевірки) та ціннісними (значущість, важливість, потрібність інформації для прийняття рішення, вартість) показниками. Вироблені на основі аналізу і синтезу розвідувальної інформації пропозиції і рекомендації для прийняття рішення становлять кінцевий інформаційний продукт – знання прогностичного характеру.

Аналітична розвідка надає можливість реалізації проактивного ризик-орієнтованого підходу у забезпеченні національної (державної) безпеки, оскільки спрямована на отримання упереджувальної інформації та прогнозування на її основі майбутнього, передусім з використанням сценарного підходу. Ефективне використання потенціалу аналітичної розвідки зменшує для спецслужби необхідність вдаватися до здійснення так званих «поліцейських» функцій, відтак відповідає Резолюції ПАРЄ № 1466 [2] та Рекомендації ПАРЄ № 1722 [3]. Крім того, спрямування «розвідки в інтересах контррозвідки» за аналітико-прогностичним вектором дозволяє уникнути конфлікту інтересів між Службою безпеки України та розвідувальними органами.

Методи аналітичної розвідки активно використовуються як спецслужбами та правоохоронними органами різних держав, так і недержавними інституціями. У багатьох країнах, зокрема у США (ФБР) й Німеччині (ВКА) були створені спеціальні підрозділи аналітичної розвідки. Прикладом результатів аналітичної розвідки є опублікований у березні 2021 року Національною радою з питань розвідки США регулярний звіт «(«Global Trends 2040: A More Contested World» [4] (публікується кожні чотири роки, починаючи з 1997-го). Автори звіту (експерти Strategic Futures Group, яка працює у складі Офісу директора Національної розвідки США) використали традиційну методологію сценарного прогнозування:

- здійснили аналіз «структурних сил» (structural forces) у чотирьох ключових галузях: демографія, навколишнє середовище, економіка, технології.
- дослідили «динаміку змін» (emerging dynamics), яка формується під впливом того, як ключові суб'єкти реагують та взаємодіють з викликами структурних сил, формуючи простір подій;
- проаналізували вплив «структурних сил» та того, як на них реагують та з ними взаємодіють суб'єкти;
- сформували п'ять потенційних сценаріїв майбутнього.

В ідеальному безпековому середовищі, досягнення якого майже не можливе, ретельний моніторинг того, як поводяться «структурні сили» та як на них реагують суб'єкти, може дати спостерігачу достатньо чіткий і надійний сигнал про те, який саме вірогідний сценарій реалізовується саме в цю хвилину. Фактичне безпекове середовище, зокрема, ймовірність впливу непрогнозованих факторів, зумовлює конвергенцію (гібридизацію) сценаріїв, що вимагає

не лише додаткового аналізу і прогнозування, але й використання інструментів аналітичної розвідки в цілях управління ризиками шляхом сприяння реалізації національних інтересів.

Слід також зазначити, що у процесі прийняття рішень стратегічного характеру у Європі та США постійно зростає важливість науково-дослідної та науково-інформаційної складової. Відповідно, у проведенні аналітичної розвідки зростає роль аналітичних центрів (think tanks) – експертних організацій, які є суб'єктами інтелектуального забезпечення державних органів влади в галузі внутрішньої та зовнішньої політики та оцінки можливих соціально-економічних наслідків політичних рішень [5]. Їх основними функціями є: аналітична, пов'язана насамперед з моніторингом, виявленням та збором інформації з ключових проблем державної політики, яка потім піддається детальному аналізу, а також з розробкою відповідного методологічного інструментарію та виробленням рекомендацій [6]; кадрова, яка забезпечується за рахунок широко розповсюдженої практики «revolving doors», тобто, переходу фахівців з «мозкових центрів» в урядовий апарат і назад у науку [7]; посередницька[8], завдяки якій подібні структури є сполучною ланкою між науковими колами та владою [9]; освітня, яка полягає не лише у просвіті та підвищенні кваліфікації управлінців, але й у проведенні наукової експертизи, а також збільшенні наукового знання з відповідних напрямів державної політики [10]. Аналітичні центри проводять аналітичну розвідку, предметом якої є відкриті дані, в інтересах урядів та спецслужб.

До напрямків діяльності таких інституцій входять, зокрема: формування ризик-орієнтованої системи забезпечення національної безпеки; прогнозування та оцінка можливих загроз національній безпеці, оцінка вразливості системи забезпечення безпеки; ідентифікація та аналіз дестабілізуючих чинників, конфлікти тощо, причин їх виникнення та їх наслідків; розроблення науково-обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів тощо.

Інтелектуальною продукцією аналітичних центрів є прикладна експертиза, рекомендації, аналітичні довідки, статті та огляди, а також фундаментальні теоретичні праці, призначені для сприяння ухваленню науково-обґрунтованих рішень державними та громадськими діячами. Згадану інтелектуальну продукцію, на відміну від власне академічних досліджень, характеризує стратегічне цілепокладання, засноване на уявленнях про бажані соціально-економічні та політичні результати, у тому числі про рівень національної безпеки. Зокрема, список програм, в рамках яких ведеться дослідницька робота RAND Corporation, включає забезпечення національної безпеки і боротьбу з тероризмом. До стратегічних програм, у рамках яких здійснюється діяльність ще одного американського аналітичного центру – Heritage Foundation,– належать, серед іншого, боротьба зі злочинністю. Міжнародний Інститут Стратегічних Досліджень Великобританії здійснює дослідницьку діяльність за сімома основними напрямами, серед яких – боротьба з тероризмом [11]. Результати аналітичної розвідки, втілені у відповідній інтелектуальній продукції, не лише забезпечують визначених законодавством суб'єктів розвідувальної і контррозвідувальної діяльності необхідною інформацією стратегічного характеру, але й можуть використовуватися ними для здійснення контрольованого інформаційного впливу на визначену аудиторію.

За даними «2020 Global Go To Think Tank Index Report» в рейтингу країн з найбільшою кількістю аналітичних центрів Україна посідала 19 місце, маючи, згідно з Доповіддю, 90 «фабрик думки» [12]. До цієї кількості увійшли недержавні установи, тому реальна кількість аналітичних центрів, з урахуванням академічних та інших науково-дослідних структур, в Україні значно вища, причому для частини з них дослідження у сфері забезпечення безпеки та протидії злочинності є профільними. Тож Україна має потенціал для створення розвиненої системи аналітичних центрів, за участю яких можна забезпечити якісне використання інструментарію аналітичної розвідки. Використання цього потенціалу сприятиме посиленню спроможностей Служби безпеки України та сектору безпеки і оборони в цілому у забезпеченні національної безпеки в умовах глобалізації та невпинного розвитку інформаційного суспільства.

Список використаних джерел:

1. Закон України «Про розвідку». URL: https://zakon.rada.gov.ua/laws/show/912–20#Text. (дата звернення 21.06.2024)
2. Резолюції ПАРЄ № 1466 «Про виконання обов'язків та зобов'язань Україною». URL: https://zakon.rada.gov.ua/laws/show/994_611#Text. (дата звернення 21.06.2024)
3. Рекомендації ПАРЄ № 1722 «Про виконання обов'язків та зобов'язань Україною». URL: https://zakon.rada.gov.ua/laws/show/994_612#Text. (дата звернення 21.06.2024)
4. Global Trends 2040. URL: https://www.dni.gov/files/ODNI/documents/ assessments/ GlobalTrends_2040.pdf. (дата звернення 21.06.2024)
5. Göran Roos. Intellectual capital analysis as a strategic tool. URL: https://www.researchgate.net/ publication/308245490_Intellectual_capital_analysis_as_a_strategic_tool. (дата звернення 21.06.2024)
6. Russell Dawson Fundamentals of Data Analytics: Learn Essential Skills, Embrace the Future, and Catapult Your Career in the Data-Driven World-A Comprehensive Guide to Data Literacy for Beginners. Jws Publishing. 168 p.
7. Natalia Bubnova. Think tanks as an actor of contemporary politics. URL: https://www. researchgate.net/publication/319949865_Think_tanks_as_an_actor_of_contemporary_politics. (дата звернення 21.06.2024)
8. Ivan Filippov. Five new roles for think tanks in the age of polycrisis. URL: https://onthinktanks. org/articles/five-new-roles-for-think-tanks-in-the-age-of-polycrisis/.(дата звернення 21.06.2024)
9. Konstantin Kurylev. Nature and key elements of the Ukrainian think tanks. URL: https://www. academia.edu/20201304/%D0%AD%D0%9A%D0%A1%D0%9F%D0%95%D0%A0%D0%A2%D0%9D%D0%9E_%D0%90%D0%9D%D0%90%D0% 9B%D0%98%D0%A2%D0%98%D0%A7%D0%95%D0%A1%D0%9A%D0%98%D0%95_%D0%A6%D0%95%D0%9D%D0%A2%D0%A0%D0%AB_%D0%9D%D0%90_%D0%A3%D0%9A%D0%A0%D0%90%D0%98%D0%9D%D0%95_%D0%A5%D0%90%D0%A0%D0%90%D0%9A%D0%A2%D0%95%D0%A0_%D0%98_%D0%9E%D0%A1%D0%9E%D0%91%D0%95%D0%9D%D0%9D%D0%9E%D0%A1%D0%A2%D0%98_NATURE_AND_KEY_ELEMENTS_OF_THE_UKRAINIAN_THINK_TANKS. (дата звернення 21.06.2024)
10. Sarah Bressan, Wade Hoxtell. Whose Bright Idea Was That? How Think Tanks Measure Their Effectiveness and Impact. URL: https://gppi.net/media/Bressan_Hoxtell_2023_Whose-Bright-Idea-Was-That.pdf.
11. Priscilla Roberts. A century of international affairs think tanks in historical perspective. URL: https://www.jstor.org/stable/24709306. (дата звернення 21.06.2024)
12. 2020 Global Go To Think Tank Index Report. URL: https://repository.upenn.edu/think_ tanks/18/.(дата звернення 21.06.2024)

РОЛЬ АНАЛІТИЧНОЇ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ У ПРОТИДІЇ ЗЛОЧИННОСТІ

Ігор ФЕДЧАК
кандидат юридичних наук, доцент
доцент кафедри інформаційного та аналітичного
забезпечення діяльності правоохоронних органів
Львівського державного університету
внутрішніх справ

Протягом останніх десятиліть правоохоронні органи зазнали фундаментальних змін в організації і тактиці застосування правоохоронних заходів упереджувальної протидії поширенню злочинності. Характерною ознакою сучасного стану справ є те, що співробітники правоохо-

ронних органів розпочали застосовувати нові, інноваційні підходи до організації правоохоронної діяльності – проактивні, які на практиці підтвердили свою результативність. Такі підходи називають проактивними моделями правоохоронної діяльності.

Основною відмінністю проактивної правоохоронної діяльності є те, що така діяльність спрямована на запобігання кримінальним проступкам, а не на реагування на наслідки вчиненого протиправного діяння. Таким чином, проактивна правоохоронна діяльність – це все, що не є реактивною правоохоронною діяльністю, і включає такі моделі: здійснення правоохоронної діяльності на основі оперативних даних (Intelligence-Led Policing / ILP); здійснення правоохоронної діяльності на основі прогнозів (Predictive Policing); здійснення правоохоронної діяльності на основі даних (Data-Driven Policing / Data-Driven Approaches to Crime and Traffic Safety / DDACTS); модель підзвітності: CompStat; здійснення правоохоронної діяльності, орієнтованої на потреби громад (Community Policing / CoP); здійснення правоохоронної діяльності, орієнтованої на певну проблематику (Problem-Oriented Policing / POP); модель профілактики скоєння тяжких злочинів через зосередження роботи поліції в місцях концентрації незначних правопорушень (модель «Broken Windows/Розбитих Вікон» (BWT)) та модель превенції злочинів за допомогою зміни навколишньої інфраструктури (Crime Prevention Through Environmental Design – CPTED). До проактивної правоохоронної діяльності також відносяться більш локальні поліцейські моделі, які ще називають концепціями, а саме: діяльність поліції у гарячих точках (Hot Spots Policing); поліцейська діяльність, заснована на доказах (Evidence-Based Policing – EBP) та концепція цілеспрямованого стримування «перетягування важелів» «Pulling Levers» Focused Deterrence. На практиці ці моделі часто тягнуть за собою дублювання застосовуваних правоохоронних стратегій і програм на місцях, наприклад, поширеним підходом до різних моделей є застосування методології аналізу проблем SARA [1]. Такі моделі мають різні стратегічні цілі (об'єкти впливу), сильні та слабкі сторони, різну мету, очікувані результати. Також моделі можуть доповнювати одна одну у випадку, якщо вони використовуються комбіновано.

Незалежно від того, застосовують проактивні моделі правоохоронної діяльності окремо чи комбіновано, аналітична розвідувальна діяльність у більшості моделей є ключовим компонентом та відіграє важливу, а у більшості моделей визначальну роль у досягненні мети упереджувального обмеження поширення злочинності. Така залежність пов'язана з тим, що визначальне значення для успішності та результативності більшості проактивних моделей правоохоронної діяльності має забезпечення якомога більшої доступності до проаналізованих досвідченими аналітиками криміногенних даних, що дозволяє розвивати поглиблене розуміння процесів (причинно-наслідкових зв'язків), що протікають у злочинному середовищі. Таке поглиблене розуміння дозволяє досягати значно вищої ефективності у реалізації оперативної, тактичної та стратегічної управлінської діяльності керівників різних рівнів правоохоронних органів по застосуванню наявних сил та засобів у напрямі обмеження поширення злочинності. Аналітична розвідувальна діяльність зосереджена, насамперед, на питаннях ідентифікації злочинців, визначенні «гарячих точок» для короткострокового реагування та підтримці традиційних тактик викриття та розслідування. Також, аналітичну розвідувальну діяльність використовують для визначення напрямів патрулювання, арешту правопорушників, інформування та запобігання кримінально-карних проявів. Проте більш ширшого запровадження потребує аналіз для підтримки керівників підрозділів і регіональних органів у плануванні заходів зі зниження рівня злочинності та розподілі ресурсів (оперативний аналіз) та аналіз спрямований на забезпечення розуміння, а також внеску у широкі стратегії, політики та ресурси (стратегічний аналіз).

Крім того, для успішної упереджувальної діяльності надзвичайно важливе значення має налагодження ефективної комунікації всередині правоохоронних структур, між такими структурами та з правоохоронними органами інших країн. Надзвичайно важливо, щоб правоохоронні органи на державному, регіональному та місцевому рівнях сприяли практиці обміну

інформацією для забезпечення реалізації спільних і комплексних заходів упереджувального реагування на кримінальна правопорушення та порушення громадського порядку, а також інші загрози стану правопорядку. Таку комунікацію якісно можуть реалізовувати підрозділи кримінального аналізу.

Урешті, надзвичайно важливо, щоб правоохоронні структури будь-якого рівня повною мірою усвідомлювали роль, навики та можливості кримінальних аналітиків, а також потенціал аналітичних продуктів, які кримінальні аналітики можуть продукувати в межах кожної з досліджуваних проактивних моделей правоохоронної діяльності.

Залучивши належно підготовлених кримінальних аналітиків, забезпечивши їх необхідними інструментами й надавши їм доступ до достовірних джерел даних, правоохоронні структури можуть отримати змогу найбільш ефективним способом реагувати на нагальні та довгострокові проблеми у межах наявних ресурсів, розуміючи глибинно причинно-наслідкові зв'язки [2, с. 557]. Крім того, завдяки аналітичній розвідувальній діяльності правоохоронні структури зможуть діяти на випередження й запобігати проблемам злочинності та порушення громадського порядку.

Попри зростаючий обсяг знань про зміст аналітичної розвідувальної діяльності та методи її проведення, майже не проведено наукових досліджень присвячених визначенню зв'язку між аналітичною розвідувальною діяльністю та зниженням рівня злочинності загалом та під час застосування проактивних підходів до організації правоохоронної діяльності. Аналітики правоохоронних органів використовують криміногенні та інші дотичні дані для проведення аналітичних досліджень із використанням спеціалізованого аналітичного програмного забезпечення, результати яких оформлюються у вигляді аналітичного звіту, досьє, профілю, орієнтування тощо. Такі аналітичні продукти надаються керівникам, які проводять ще один рівень аналізу і визначають тактику застосування сил та засобів (ресурсів) щоб більш ефективно вирішувати ідентифіковані проблеми та ризики їх виникнення. Таким чином, незважаючи на те, що продукти аналітичної розвідувальної діяльності можуть бути точними та високоякісними, успіх у обмеженні поширення злочинності залежить від обраної тактики дій конкретного керівника. Отже, роль технологій, аналітичних програм, методів та технік проведення аналітичних досліджень криміногенних даних і самих аналітиків правоохоронних органів у виборі заходів протидії проблемам та їх успішному впровадженні є надзвичайно обмеженою. Таким чином, не можна сказати, чи аналітична розвідувальна діяльність запобігає або вирішує різні проблеми злочинності, проте можна говорити лише про те, що це важливий, а в деяких випадках і необхідний компонент організації проактивної правоохоронної діяльності.

Список використаних джерел:

1. Федчак І. А. Практичні аспекти вирішення проблем за методологією SARA під час реалізації моделі правоохоронної діяльності, орієнтованої на потреби громад (Community Policing). Актуальні проблеми держави і права 2023. № 99. С. 140–146. DOI: https://doi.org/10.32782/apdp.v99.2023.20.

2. Федчак І. А. Концептуальні основи та науково-практичні аспекти проактивних моделей правоохоронної діяльності: монографія. Львів: Львівський державний університет внутрішніх справ, 2024. 628 с.

ПРО ДЖЕРЕЛА ІНФОРМАЦІЇ В СИСТЕМІ АНАЛІТИЧНОЇ РОЗВІДКИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Андрій ХАНЬКЕВИЧ
старший викладач Національного
юридичного університету імені Ярослава Мудрого

У контексті оперативно-розшукової, контррозвідувальної та кримінальної процесуальної діяльності органів і підрозділів Служби безпеки України (далі – СБУ) термін «аналітична розвідка» використовується для позначення такої діяльності, в якій застосовуються аналітичні методи для збору, обробки та інтерпретації інформації, яка має значення для виконання покладених на відповідні служби та підрозділи завдань.

Цей термін використовується у контексті національної безпеки та оборони, де аналітична розвідувальна діяльність часто є фундаментом для підготовки стратегій і тактик протидії потенційним загрозам, які можуть мати різні форми агресії: військові, терористичні, інформаційні, економічні, політичні, екологічні тощо.

Ці форми агресії можуть здійснюватися окремо або в поєднанні, а їх виявлення та запобігання важливі для забезпечення національної та міжнародної безпеки.

Інформаційна складова відіграє ключову роль у протидії зазначеним викликам. В аспекті вирішення завдань органами і підрозділами СБУ особливе місце займає інформаційна потреба. Інформаційна потреба за своєю природою динамічна. Вона постійно змінюється під впливом зовнішнього середовища, конкретизації завдань, зміни напряму та інструментарію інформаційного пошуку [1].

Мотиви інформаційної потреби СБУ віддзеркалюються у напрямах її оперативно-розшукової, контррозвідувальної та кримінальної процесуальної діяльності, що спонукає до використання різноманітних джерел інформації для вирішення поставлених завдань. Основою цього процесу є систематичне визначення або встановлення необхідних інформаційних джерел, безпосередньо отримання інформації, її упорядкування, аналіз, розповсюдження результатів та прийняття відповідних управлінських рішень, спрямованих на виконання конкретних завдань органами та підрозділами протидіючих сил.

Актуальність дослідження класифікації джерел інформації зумовлена потребою у створенні впорядкованого підходу до організації та розподілу різноманітної інформації, яка виникає в процесі роботи органів і підрозділів СБУ. Це дозволяє ефективніше збирати, оновлювати та використовувати цю інформацію в інтересах Служби.

Для створення ефективної класифікації важливо враховувати принцип зв'язку між вибраними об'єктами. Це означає, що необхідно чітко визначити основні властивості об'єкту, провести його аналіз та синтез у взаємозв'язку з іншими об'єктами [2, с. 21]. Основне ж завдання класифікації полягає у виявленні типових об'єктивних ознак, на підставі яких можна групувати об'єкти, що класифікуються, та визначати їх місце у множині. Однак, в процесі класифікації особливу увагу слід приділити розподілу об'єктів за подібністю та відмінностями залежно від обраного критерію [3, с. 15]. Однією з головних умов будь-якої класифікації є вибір правильного критерію, який дозволяє зберегти всі суттєві ознаки основного явища і водночас виокремити додаткові ознаки, що відрізняють класи від інших.

Розроблення класифікації джерел інформації в аналітичній розвідці СБУ передбачає кілька важливих цілей, а саме:

- систематизація джерел, що дозволяє визначити придатність різних джерел для конкретних завдань, підвищуючи якість та об'єктивність аналітичних звітів;
- оптимізація збору та аналізу інформації, що допомагає визначити пріоритетність джерел, забезпечуючи швидке та ефективне виявлення загроз та розробку протидіючих стратегій;

– уніфікація методів дослідження, як передбачає групування джерел за основними ознаками, що дозволяє застосовувати однакові або схожі методи дослідження, враховуючи, що значення ознак може змінюватися залежно від поставлених завдань.

Джерела інформації в аналітичній розвідці є ресурсами первинних даних або іншої інформації для аналізу. Вони можуть включати текстові документи, статистичні дані, відео та аудіозаписи, електронні повідомлення, кореспонденцію, свідчення, звіти, соціальні медіа тощо. До основних типів джерел інформації для потреб СБУ переважно належать: 1) людина; 2) документ; 3) комп'ютерні бази даних.

Людина як ключове джерело інформації для СБУ – це особа з доступом до відкритої, конфіденційної або секретної інформації. Такі особи можуть діяти як очевидці, свідки, агенти чи фігуранти розслідувань. Вони належать до різних сфер суспільного життя, включаючи політику, бізнес, науку та культуру, і можуть надавати цінні дані та орієнтуючу інформацію, що допомагає СБУ у розслідуваннях та запобіганні загрозам національній безпеці, наприклад: політичні діячи та державні чиновники; представники бізнесу та інвестори; активісти громадських організацій та правозахисники; журналісти та блогери; відомі діячи культури тощо. Осіб зазначеної категорії об'єднує те, що вони мають доступ до цінної інформації, а також мають значний вплив на суспільні процеси. Їхні зв'язки, знання та позиції дозволяють їм збирати, передавати та аналізувати важливі дані, що робить їх важливими джерелами інформації для СБУ в контексті забезпечення національної безпеки.

Документ, як важливе джерело інформації може бути визначений як будь-який письмовий, електронний або інший носій інформації, який містить дані про події, осіб, організації, або інші факти, що можуть бути корисними для розвідувального аналізу в діяльності СБУ. Документи можуть бути отримані з внутрішніх архівів державних органів, установ та організацій різної форми власності, а також формуватися через опрацювання результатів діяльності інших джерел. Аналіз документів дозволяє органам та підрозділам СБУ вчасно виявляти потенційні загрози та ризики в середовищі функціонування Служби, розробляти стратегії протидії, планувати заходи у сферах оперативно-розшукової, контррозвідувальної та кримінальної процесуальної діяльності тощо.

Серед найбільш часто використовуваних в аналітичній розвідувальній діяльності можна виділити такі види документів:

1) нормативно-правові документи органів державної влади (регулюють суспільні відносини та встановлюють правові норми. Вони можуть прийматися на різних рівнях влади і включають закони, укази, постанови, розпорядження та інструкції. Аналіз таких документів в аналітичній розвідці СБУ дозволяє глибше розуміти правові вимоги, виявляти потенційні загрози національній безпеці, оцінювати їхній вплив і розробляти стратегії протидії. Також ці документи відображають тенденції розвитку суспільства і політичні орієнтири, що сприяє прогнозуванню змін у політиці країни та реагуванню на загрози. Аналіз нормативно-правових актів допомагає виявляти шляхи впливу на процеси управління та прийняття рішень, що є важливим для формування стратегічних планів СБУ);

2) установчі документи (дозволяють розуміти цілі та стратегії досліджуваних об'єктів; відображають історичний контекст, цілі, завдання та їх стратегічні пріоритети; дозволяють виявляти слабкі місця та вразливості в діяльності об'єктів дослідження; допомагають у визначенні ключових фігурантів та можливі джерел впливу або конфліктів, що сприяє виявленню можливостей для співпраці);

3) статистичні дані (відомості, що відображають аспекти соціально-економічного, демографічного, політичного та інших сфер життя суспільства й сприяють розумінню, наприклад, стану виробництва, споживання, безробіття, інвестицій тощо, тобто допомагають розуміти стан економіки, виявляти вразливості або можливості для впливу; дозволяють розкривати демографічні тенденції та їх наслідки для соціально-політичної ситуації; дозволяють відстежувати та аналізувати соціальні процеси та їх наслідки; оцінювати політичних ризиків та можливості, на підставі аналізу статистичних даних про виборчі процеси, громадські настрої, рівень задоволеності політичними лідерами тощо;

4) матеріали мас-медіа (відображають громадську думку, настрої та ставлення громадян до різних подій, явищ та осіб. Аналіз цих матеріалів дозволяє визначити тенденції у громадському мисленні та реакцію на певні події. Мас-медіа можуть розкривати ключові проблеми, тренди та події у суспільстві, економіці та політиці. Аналітичний підхід до мас-медіа допомагає виявляти потенційні проблеми та можливості для стратегічного впливу, а також розкривати стратегії та тактики медіаполітики різних суб'єктів, включаючи уряди, політичні партії, корпорації та інші організації);

5) аналітичні звіти та дослідження (надають об'єктивні дані про суспільне, економічне, політичне життя та безпеку держави; містять систематизовані та проаналізовані дані з різних джерел, що допомагають розкривати основні тенденції, проблеми чи можливості в певних сферах; використовуються для аналізу соціальних та економічних тенденцій, політичної ситуації, потенційних безпекових загроз, а також для розуміння політичної стабільності та нормалізації обстановки; у рамках зовнішньої політики держави дозволяють аналізувати динаміку міжнародного середовища, виявляти можливості для співпраці та напрями нейтралізації конфліктів);

6) документи, створені за результатами проведення оперативно-розшукових, контррозвідувальних заходів (використовуються для оцінки загроз національній безпеці, виявлення злочинних структур, аналізу внутрішніх загроз та моніторингу зовнішніх загроз (діяльність іноземних розвідувальних служб, кібератаки тощо);

7) документи, створені у процесі досудового розслідування кримінальних проваджень (використовуються для аналізу модусів злочинності, виявлення злочинних структур, встановлення осіб, причетних до протиправної діяльності, оцінки ефективності дій оперативних підрозділів та слідчих органів; можуть містити інформацію про потенційні загрози національній безпеці).

Комп'ютерні бази даних – це автоматизовані та структуровані системи для зберігання та організації інформації з можливістю доступу, пошуку та аналізу, які організовані за різними критеріями, такими як тематика подій, хронологія та джерела. Призначені для оперативного аналізу ситуацій, виявлення потенційних загроз та розроблення стратегій протидії. Сприяють прийняття ефективних управлінських рішень в інтересах національної безпеки України.

Таким чином, наукове дослідження джерел інформації в системі аналітичної розвідки є критично важливим для діяльності органів і підрозділів СБУ. Знання й використання відповідних знань забезпечує доступ до об'єктивних, структурованих та обґрунтованих даних, необхідних для всебічного аналізу суспільних, економічних, політичних та безпекових аспектів, що впливають на національну безпеку, дозволяє виявляти та розуміти основні тенденції, оцінювати різноманітні загрози, аналізувати й нейтралізувати внутрішні і зовнішні загрози.

Список використаних джерел:

1. Конкурентна розвідка: навч. посіб. / І. Копотун та ін. Ірпінь: Ун-т ДФС України, 2020. 188 с.

2. Адамова О. Поняття правової класифікації. Часопис цивілістики, 2015. Вип. 18. С. 19–24.

3. Кривоченко Л. Классификация преступлений. Х.: Вища школа, 1983. 129 с.

Наукове видання

СБУ В УМОВАХ ВІЙНИ В УКРАЇНІ: СУЧАСНІ РЕАЛІЇ ТА ІННОВАЦІЙНІ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Матеріали міжнародної науково-практичної конференції 4–5 липня 2024 року

Відповідальний за випуск	О. В. Діордійчук
Комп'ютерна верстка	Д. М. Алексєєв
Обкладинка	Д. М. Алексєєв

Підписано до друку 02.07.2024 р. Формат 60 х 84 $^{1}/_{8}$.
Папір офсетний. Гарнітура «Times New Roman».
Друк офсетний. Умовн.-друк. арк. 34,64.

Видавництво «Алерта»
04210, м. Київ, а/с 112.
Тел.: (044) 223-15-25, (099) 607-97-62.
E-mail: alerta.pravovaednist@gmail.com, веб-сайт: alerta.kiev.ua
Свідоцтво суб'єкта видавничої справи ДК № 788 від 29.01.2002 р.