НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЯРОСЛАВА МУДРОГО

ІНСТИТУТ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

АКТУАЛЬНІ ПИТАННЯ ДОКАЗУВАННЯ ПО ЗЛОЧИНАМ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Матеріали Всеукраїнського круглого столу
(23 листопада 2024 року)

Харків 2025

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЯРОСЛАВА МУДРОГО

ІНСТИТУТ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

АКТУАЛЬНІ ПИТАННЯ ДОКАЗУВАННЯ ПО ЗЛОЧИНАМ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Матеріали Всеукраїнського круглого столу
(23 листопада 2024 року)

Харків
2025

УДК 343.14.

Рекомендовано до видання Вченою радою
Інституту Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого,
протокол засідання від 22.01.2025 № 35

Актуальні питання доказування по злочинам проти основ національної безпеки. Матеріали Всеукраїнського круглого столу, 23 листопада 2024 р.; м. Харків. / Редкол.: О. Червяков, О. Метелев, А. Когут. – Х., 2025. — 100 с.

Збірник містить тези доповідей і виступів науковців, практичних працівників та курсантів, присвячених: проблемам збору та фіксації доказів органами Служби безпеки України проти основ національної безпеки, зокрема в цифровому середовищі; питанням трансформації злочинності, пов’язаної з її інтеграцією в кібервсесвіт як і з позиції вчинення кримінальних правопорушень, так і приховування слідів злочинів; а також основам власної кібербезпеки органів державної влади, установ, організацій та громадян.

Для співробітників органів сектору безпеки, науковців, викладачів, курсантів й студентів вищих юридичних навчальних закладів.

Адреса Інституту: 61002, м. Харків, вул. Мироносицька, 71,
Телефон / факс: (057)700-34-55
E-mail: ipuk@ssu.gov.ua

ЗМІСТ

ВІТАЛЬНЕ СЛОВО !

Шановні учасники круглого столу

«Актуальні питання доказування по злочинам проти основ національної безпеки»

Шановні колеги, я хотів би привітати на нашому вже традиційному заході всіх: науковців, правників, співробітників Служби, діючих і майбутніх, а також всіх хто доєднався до нашої зустрічі. Це вже другий такий круглий стіл, який ми запроваджували, як площадку де мають обговорюватись актуальні питання не тільки кримінального права та кримінального процесу у контексті реалізації завдань Служби безпеки України, але й інші проблемні питання, зокрема питання впливу цифровізації на кримінальне законодавство, проблем доказування по злочинам, вчинених у цифровому середовищі, розуміння інструментів та особливостей функціонування кіберпростору та забезпечення власної кібербезпеки. Нашою метою є не лише вирішення питання пошуку та фіксації доказів у кібернетичному просторі, але й надання цінних знань для використання в побуті та службовій діяльності, безпосередньо не пов'язаній з кримінальним процесом, адже цифровізація суспільства торкається кожного, а великий масив суспільних відносин переміщається у кібернетичний простір. Все це, на наш погляд, дуже важливо, і поєднання наукової думки і досвіду з практикою «в полі», думаю, дозволить нам, в Інституті СБУ, створювати і запроваджувати саме такі навчальні програми і контент, які дозволять формувати як у курсантів, так і у діючих співробітників, спеціальні компетентності, які дозволятимуть ефективно вирішувати завдання і розслідувати злочини, віднесені до підслідності Служби.

Це особливо важливо зараз, в умовах війни росії проти України, коли кожний належним чином зафіксований і процесуально задокументований факт злочину проти наших людей і нашої держави може наблизити притягнення російських злочинних очільників і виконавців до невідворотного покарання. Саме невідворотність покарання злочинця за скоєний злочин є основним запобіжником, основною профілактикою злочинності.

Саме тому, ми повинні у своїй справі бути професіоналами і з кожним днем, роблячи начебто буденні, але дуже важливі кроки, опановуючи і застосовуючи на практиці отримані знання і інструменти, наближати нашу Перемогу і Мир у нашій державі. Отже, запрошую всіх учасників круглого столу під час проведення заходу долучатись до дискусії, шукати шляхи вирішення існуючих проблемних питань та моделювати кримінальну процесуальну науку майбутнього.

ЧЕРВЯКОВ Олександр Іванович, Начальник Інституту Служби безпеки України Національного юридичного університету імені Ярослава Мудрого, кандидат юридичних наук

Капліна Оксана Володимирівна
докторка юридичних наук, професорка,
завідувачка кафедри кримінального процесу
Національного юридичного університету
імені Ярослава Мудрого

ПРОВОКАЦІЯ ВЧИНЕННЯ ЗЛОЧИНУ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Відповідно до ст. 2 Кримінального процесуального кодексу України (далі - КПК) завданнями кримінального провадження є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура [1]. Належність процедури здійснення кримінального провадження означає, що слідчі (розшукові) дії, негласні слідчі розшукові дії, інші процесуальні дії мають вчинятися відповідно до передбаченої форми кримінального провадження, з неухильним додержанням вимог Конституції, кримінального процесуального законодавства, міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. На необхідність додержання вимог, встановлених КПК, неодноразово вказує КПК України у ст. 9, 25, 36, 86, 271 тощо. Таким чином законодавець наголошує на аксіологічному значенні кримінальної процесуальної форми, що a priori здатно забезпечити права та законні інтереси осіб, які беруть участь у кримінальному провадженні, допустимість отриманих доказів, ефективність кримінальної процесуальної діяльності та зрештою досягнення завдань кримінального провадження.

Однак у правозастосовної практиці непоодинокими є випадки, коли органи досудового розслідування нехтують вимогами кримінального процесуального закону, припускаються порушення вимог КПК, вдаються до провокування (підбурювання) до вчинення кримінальний правопорушень. Проблема ускладняються тим, що законодавство не містить визначення поняття провокації та тих критеріїв, які здатні відмежувати законну діяльність з фіксації вчинюваних кримінальних правопорушень та провокування до їх вчинення. Єдина згадка стосовно заборони провокації міститься у ст. 271 КПК «Контроль за вчиненням злочину» частина 3 якої передбачає, що «під час підготовки та проведення заходів з контролю за вчиненням злочину забороняється провокувати (підбурювати) особу на вчинення цього злочину з метою його подальшого викриття, допомагаючи особі вчинити злочин, який вона би не вчинила, якби слідчий цьому не сприяв, або з цією самою метою впливати на її поведінку насильством, погрозами, шантажем. Здобуті в такий спосіб речі і документи не можуть бути використані у кримінальному провадженні».

Незважаючи на те, що ст. 271 КПК логічний акцент робить на заборону провокувати особу, нормативний зміст цієї статті дозволяє виокремити ознаки провокації. Зокрема: 1) вона можлива під час підготовки та проведення заходів з контролю за вчиненням злочину; 2) суть її полягає в підбуренні (провокуванні, спонуканні) особи на вчиненні злочину, допомозі, сприянні їй його вчинити; 3) підбурення справило такий вплив на особу, що вона вирішила вчинити злочин, чого б вона не зробила, якби не було вказаного впливу; 4) можливим є застосування впливу шляхом насильства, погроз шантажу; 5) мета зазначеного психологічного чи фізичного впливу – подальше викриття особи у вчиненні злочину.

Оскільки вітчизняна практика доказування провокації вчинення злочину лише починає формуватися, доцільним є звернення до рішень Європейського суду з прав людини (далі – ЄСПЛ), який за два десятка років напрацював підходи щодо кваліфікації провокації злочину, які допоможуть відмежувати підбурювання від законних дій, спрямованих на викриття злочину або особи, яка його вчиняє. Зокрема, це такі справи, як «Тейкшейро де Каштро проти Португалії» (Teixeira de

Castro v. Portugal) від 9 червня 1998 р. скарга № 44/1997/828/1034 (перша справа щодо провокації ЄСПЛ); «Секейра проти Португалії» (Sequeira v. Portugal) від 6.05.2003 р. скарга № 73557/01 №73557/01; «Эдвардс и Льюис проти Об'єднаного Королівства» (Edwards and Lewis) від 27 жовтня 2004 р, скарги № 39647/98, 40461/98; «Еврофінаком против Франции" (Eurofinacom v. France) скарга № 58753/00, 2004-VII; «Шеннон проти Об’єднаного королівства» (Shannon v. United Kingdom), скарга N 67537/01 від 6 квітня 2004; «Ваньян проти Росії» (Vanyan v. Russia) від 15 грудня 2005 р., скарга № 53203/99; «Худобін проти Росії» від 26 жовтня 2006 р. скарга № 59696/00; «Раманаускас проти Литви» №1 від 5 лютого 2008 р, скарга № 74420/01; «Малінінас проти Литви» (Malininas v. Lithuania) від 1 липня 2008 р., скарга № 10071/04; «Барак Хан проти Туреччини (Burak Han v. Turkey) від 15 грудня 2009 р., скарга № 17570/04№; «Барак Хан проти Туреччини (Burak Han v. Turkey) від 15 грудня 2009 р., скарга № 17570/04; «Веселов та інші проти Росії» від 2 жовтня 2012 р., скарги № 23200/10, 24009/07, 556/10; «Сепіл проти Туреччини (Sepil v. Turkey) від 12 грудня 2013 р., скарга № 17711/0347; «Давитидзе против России» від 30 травня 2013 р. , скарга № 8810/05; «Санду та інші проти Молдови (Sandu and Others v. Moldova) №16463/08 від 11 лютого 2014 р.; «Лагутін та інші проти Россії» (Lagutin and Others v. Russia) від 24 квітня 2014 р., скарги № 6228/09, 19123/09, 19678/07, 52340/08 и 7451/09; «Фюрч проти Німеччини» (Furcht v. Germany) № 54648/09 від 23.10.2014 р.; «Носко і Нефьодов проти Росії» (Nosko and Nefedov v. Russia) №5753/09, №11789/10 від 30.10.2014; «Волков и Адамский проти Росії» від 26 березня 2015 р, скарги № 7614/09, 30863/10; «Таранекс проти Латвії» (Taraneks v. Latvia) №3082/06 від 02.12.2014 р.; «Кіпріан Владут и Іоан Флорін Поп (CiprianVlăduț and Ioan Florin Pop) проти Румунії від 16 липня 2015 р., скарга № 43490/07 та 44304/07; «Матанович проти Хорватії» (Matanović v. Croatia) №2742/12 від 04.04.2017; «Раманаускас проти Литви №2» (Ramanauskas v. Lithuania (№2) №55146/14 від 20.02.2018; «Чохонелідзе проти Грузії» (Tchokhonelidze v. Georgia) №31536/07 від 28.06.2018; «Акбай та інші проти Німеччини» (Akbay and others v. Germany) від 15.10.2020 заява № 40495/15 and Final 15/01/2021; «Кузьмина та інші проти Росії від 20 квітня 2021 р., справа № 66152/14 (системна проблема) тощо.

Що стосується України, то перша справа «Яхимович проти України» була ухвалена 16 грудня 2021 року (справа № 23476/15, остаточне 9 травня 2022 р.). Щоправда стосовно України подавалися ще 3 скарги до ЄСПЛ, однак всі вони були визнані неприйнятними. Це зокрема, справа Любченко проти України (Leyubchenko v. Ukraine) № 34640/05, 31/05/2016; Берлизев проти України (Berlizev v. Ukraine) № 43571/12, 08/08/2021 (неприйнятність); Волков проти України заява № 74785/1428 від 28.03.24 р.

Узагальнення практики ЄСПЛ дозволяє зробити акцент на декількох важливих моментах.

Перший полягає в тому, що Конвенція про захист прав людини і основоположних свобод [2] в принципе не забороняє використання анонімної інформації на стадії розслідування кримінальної справи там, де характер злочину цього потребує. Разом з тим, хоча зростання організованої злочинності, безсумнівно, зумовлює застосування відповідних заходів, право на справедливий розгляд залишається на першому місці і не може бути принесене в жертву доцільності, а відтак використання негласних агентів має бути обмеженим і забезпеченим гарантіями навіть у справах, пов'язаних із боротьбою з торгівлею наркотиками (§ 35-36 справа «Тейкшейро де Каштро проти Португалії»).

Такий підхід про пріоритетність забезпечення права особи на справедливий суд, яке безумовно порушується під час провокування (підбурювання) особи на вчинення злочину, ЄСПЛ підтверджував неодноразово. Зокрема, у справі «Банніков проти Росії» він зазначив, що враховуючи специфіку слідчих заходів, що проводяться з метою боротьби з незаконним обігом наркотиків та корупцією, позицією ЄСПЛ, що вже давно сформувалася, є те, що державні інтереси не можуть обґрунтовувати використання доказів, отриманих внаслідок поліцейської провокації, оскільки застосування таких доказів піддає обвинуваченого ризику остаточно втратити справедливий судовий розгляд з самого початку (§ 33).

Другий важливий момент полягає в тому, що ЄСПЛ послідовно та поступово в низці справ розробив матеріальний та процесуальний тест на провокацію. Підходи щодо змістовного усвідомлення матеріальних ознак провокації були вказані вже в

першому рішенні ЄСПЛ щодо провокації в 1998 році, однак узагальнені у справі «Баннікова проти Росії», та згодом систематизовані у справі «Матанович проти Хорватії». Сутність двох тестів на провокацію полягає в тому, що при заяві сторони захисту в судовому розгляді про провокування (підбурення) з боку органів, які здійснювали досудове розслідування, суд має обов'язково перевірити таку заяву. Матеріальний тест дозволить встановити – чи є змістовні ознаки провокації (чи були в наявності дії, які можна кваліфікувати як підбурення). В свою чергу процесуальний тест розроблений ЄСПЛ для того, що б перевірити процесуальний аспект здійснення досудового та судового провадження. Зокрема, чи були підстави для проведення негласних заходів, чи були вони вчинені під контролем суду; чи була заява про провокацію перевірена судом в змагальному процесі; чи навела сторона обвинувачення доводи на підтвердження позиції щодо відсутності провокування.

Третій важливий момент полягає в тому, що в справі «Раманаускас проти Литви» у п. 55 ЄСПЛ сформулював поняття провокації: «55. Поліцейська провокація має місце тоді, коли відповідні посадові особи - чи то співробітники сил безпеки, чи то особи, які діють за їхніми вказівками, - не обмежуються розслідуванням злочинної діяльності в основному пасивним способом, а здійснюють такий вплив на суб'єкта, що підбурює до вчинення злочину, який в іншому випадку не був би вчинений, з метою уможливлення встановлення факту злочину, тобто надання доказів і порушення кримінального переслідування.» Це рішення, безумовно, було одним з тих ключових рішень, які змінили в тому числі кримінальний процес України, а підходи ЄСПЛ були враховані в КПК 2012 року.

Четвертий момент полягає в тому, що усвідомлюючи підходи щодо провокації треба звернутися до справи «Лагутін та інші проти Росії» та, зокрема, окремій думці судді ЄСПЛ від Португалії Пауло Пінто де Альбукерке, який, аналізуючи справу, на підставі існуючих європейських стандартів розробив та запропонував рекомендації для держав, відповідно до яких треба будувати національне законодавство [3, с. 348-353]. Формат виступу на конференції не дає можливості навести всі позиції, але звернення до першоджерела дозволить правозастосовникам та законотворцям будувати законодавство та правозастосовну практику з

урахуванням підходів, які здатні забезпечити дотримання прав людини, збирання допустимих доказів та здійснювати боротьбу із злочинністю відповідно до сучасних підходів. Наприклад, серед іншого суддя ЄСПЛ вказав, що сумісне з правами людини законодавство про «особливі методи розслідування» повинно мати, як мінімум, такі ознаки: (1) Закон мусить містити перелік тяжких злочинів, які можуть розслідуватися за допомогою особливого методу розслідування, це стосується переліку конкретних злочинів або загальної вказівки на злочини, за вчинення яких передбачене покарання у виді позбавлення волі не менше ніж на чотири роки. (2) Закон має передбачати перелік спеціальних методів розслідування, таких як перевірочні закупки, контрольований продаж, контрольований імпорт, контрольований експорт, контрольований транзит, інші контрольовані операції, впровадження та інші негласні операції. (3) Закон повинен передбачати перелік осіб, які можуть застосовувати особливі методи розслідування, серед яких співробітники поліції, митники та інші співробітники правоохоронних органів або приватні особи, які діють за вказівкою правоохоронних органів. (4) Закон має встановлювати максимальну тривалість особливих методів розслідування, яка може бути подовжена один або декілька разів після оцінки компетентними органами результатів початкових стадій операції, але в будь-якому випадку за наявності максимального строку, встановленого для всієї операції. (5) Закон повинен вказувати «достатні підстави», що можуть виправдовувати використання особливого методу розслідування, такі як забезпечення правопорядку, запобігання злочинам та здійснення переслідування. (6) Закон також мусить відповідати критеріям співмірності: 1) особливі методи розслідування мають бути співмірними зазначеним «достатнім підставам», що вимагає встановлення справедливого балансу між конкуруючими інтересами підозрюваного і «достатніми підставами», наведеними в обґрунтування особливого методу розслідування; 2) встановлення рівноваги також має брати до уваги права та інтереси ймовірних потерпілих, а отже, наприклад, у справах про торгівлю людьми недоцільна контрольована поставка; 3) чим більш серйозні передбачувані злочини та їх минулі або майбутні наслідки, тим більш інтрузивним і екстенсивним може бути особливий метод розслідування; 4)

особливий метод розслідування має забезпечити дотримання мінімальних прав підозрюваних, таких як право на життя й здоров'я.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України від 13.04.2012 р. No 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17/ed20220520#Tex (дата звернення 1.12.2024)

2. Конвенція про захист прав людини і основоположних свобод від 4.11.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення 1.12.2024)

3. Пінто де Альбукерке Пауло. Окрема думка. Шлях до справедливості / Пауло Пінто де Альбукерке ; [пер. з англ. та фр. В. А. Капліної ; упоряд., авт. передм. О. В. Капліна]. – Харків : Право, 2020. – 552 с.

ТОРБАС Олександр Олександрович

доктор юридичних наук, професор,

Національний університет «Одеська юридична академія»

ОСОБЛИВОСТІ ЗБИРАННЯ ДОКАЗІВ З ВІДКРИТИХ ДЖЕРЕЛ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

На сьогодні відбувається досить стрімкий розвиток новітніх технологій, який в тій чи іншій мірі стосується всіх сфер нашого життя. Не стало виключенням і галузь кримінального процесу. В силу технологічних трансформацій від осіб, уповноважених на розслідування, розгляд та вирішення кримінальних правопорушень, вимагаються нові навички, які в першу чергу пов'язані з виявленням та фіксацією доказів, які в подальшому можуть бути використані в кримінальному провадженні. З урахуванням величезного обсягу інформації, який на даний момент знаходиться у вільному доступі в мережі Інтернет, знайти відомості, які стосуються певних осіб чи подій, стало набагато легше. Така доступність

використовується як зловмисниками, так і самими працівниками правоохоронних органів, які можуть збирати доказову інформацію з відкритих джерел. В той же час галузь кримінального процесу є вкрай забюрократизованою, а тому будь-яке збирання доказів має відбуватися в тому порядку, який передбачений чинним кримінальним процесуальним законодавством України. І саме в сфері кримінального процесу існують певні складнощі із збиранням та подальшим використанням таких доказів.

В першу чергу необхідно зазначити, що на відміну від інших процесуальних кодексів, КПК України не оперує таким поняттям як «електронні докази». Проблема полягає в тому, що на даний момент більшість відкритих джерел знаходяться саме в мережі Інтернет, а тому фіксація таких відомостей так чи інакше буде пов'язана з електронними доказами. З урахуванням обмеженої кількості джерел доказів і теоретики [1], і практики в цілому одноголосно підтримують позицію, що в кримінальному процесі електронні докази необхідно розглядати як документи. «Отримання доказів із відкритих джерел – питання не нове для українських судів. Уже тривалий час у деяких кримінальних провадженнях, не тільки за КПК України 2012 року, а в окремих випадках і за КПК 1960 року, були електронні докази. Слідство та суди використовують ці докази відповідно до §1 «Поняття доказів, належність та допустимість при визнанні відомостей доказами» гл. 4 «Докази і доказування» КПК України, ст. 99 «Документи» цього Кодексу» [2].

В цілому необхідно зазначити, що докази, отримані з відкритих джерел, досить давно та досить активно застосовуються в правозастосовчій практиці. Так, відомості, отримані за допомогою OSINT, використовуються для обґрунтування клопотань про проведення обшуку («також, за допомогою відкритих джерел інформації всесвітньої мережі Інтернет, методом OSINT, здійснено перевірку абонентського номеру мобільного зв`язку НОМЕР_2 з метою встановлення інформації про особу користувача. Таким чином, в ході проведених заходів, встановлено особу, причетну до вчинення вищевказаного кримінального правопорушення, а саме: ОСОБА_7 , ІНФОРМАЦІЯ_1, ІПН НОМЕР_5, зареєстрований та проживає за дресою: АДРЕСА_1 , користується абонентським

номером мобільного телефону НОМЕР_6» [3]), накладення арешту на майно («… після чого оперативним шляхом за допомогою відкритих джерел інформації та баз даних, проведено моніторинг мережі Інтернет та перевірки за наявними обліками ДКП, додатково із використанням програмного забезпечення для аналізу даних та інструменту OSINT «ІНФОРМАЦІЯ_3 », у результаті чого встановлено особу: ОСОБА_6 ІНФОРМАЦІЯ_4, адреса мешкання: АДРЕСА_1, тел.: НОМЕР_1» [4]) та навіть встановлення факту смерті («Суд вважає, що у зв`язку з тимчасовою окупацією м. Сватово Луганської обл. неможливо зареєструвати смерть ОСОБА_3 в органах РАГС і в даному випадку можливо на підтвердження смерті ОСОБА_3 прийняти ті відомості, які зазначені прокурором за посиланням ІНФОРМАЦІЯ_5, як інформацію з відкритих джерел (OSINT)» [5]), чого було достатньо для закриття кримінального провадження. При цьому на відомості з відкритих джерел посилаються не лише сторони кримінального провадження, а і самі судді, коли перевіряють докази, які їм були надані («Крім того, в клопотанні прокурора зазначена адреса за реєстрації власника майна: АДРЕСА_1 , яка згідно даних з відкритих джерел не існує» [6]).

Ігнорувати значення та можливості застосування відомостей, отриманих з відкритих джерел, на даний момент неможливо. В той же час необхідно констатувати, що на практиці досі існують проблеми, які пов’язані зі збиранням доказів з відкритих джерел.Так, посилання лише на ст. 99 КПК України не вирішує низку питань, які пов’язані зі збиранням таких доказів. В першу чергу необхідно встановити, хто саме уповноважений на їх збирання. З одного боку відомості знаходяться у вільному доступі, будь-хто може з ними ознайомитися, зафіксувати та в подальшому посилатися на них. З іншого – відповідно до ч. 1 ст. 93 КПК України, збирання доказів здійснюється сторонами кримінального провадження, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, у порядку, передбаченому КПК України. З урахуванням того, що належний суб’єкт збирання є одним з критеріїв оцінки допустимості доказів, вкрай важливо, щоб в ході оцінки відповідних доказів у уповноважених суб’єктів не виникали сумніви щодо того, чи міг відповідний учасник кримінального провадження відповідні докази збирати.

Навіть не зважаючи на те, що відповідні докази знаходяться у відкритих джерелах і будь-який уповноважений чи неуповноважений учасник кримінального провадження може з ними самостійно ознайомитись, при оцінці доказів обов’язково має бути встановлено, що в межах саме кримінального провадження вони були отримані належним суб’єктом.

Відповідно, в кримінальному провадженні такі докази мають збиратися або слідчим, дізнавачем чи прокурором, або оперативними підрозділами, проте лише за дорученням в порядку ст. 41 КПК України. «Електронні (цифрові) докази, до яких належать матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані), що містяться у відкритих (інтернет, різноманітні засоби масової інформації, соціальні мережі) чи закритих мережах (приватні месенджери та телеграм- канали, особисте листування з використанням комп'ютерної техніки і мобільних телефонів, флешнакопичувачі, карти пам'яті тощо), у яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог процесуального законодавства, є основними доказами у кримінальних провадженнях щодо злочинів проти основ національної безпеки України… За змістом ст. 99 КПК матеріали, у яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог процесуального законодавства, є документами та можуть використовуватися в кримінальному провадженні як докази… Як убачається з матеріалів кримінального провадження, на виконання відповідних доручень старшого слідчого, наданих у порядку ст. 40 КПК, оперуповноважений співробітник провів огляд інтернет-сторінок, зроблено скриншоти і завантажено відеофайли, які є додатками до протоколів огляду, оформлених, відповідно до вимог КПК» [7].

Іншим важливим питанням є особливості фіксації таких доказів. З попереднього прикладу можна побачити, що на практиці докази з відкритих джерел фіксуються за допомогою такої слідчої (розшукової) дії як огляд веб-сторінки. І хоча саме ця дія є вкрай актуальною та вживаною, її складно назвати найкращим способом для фіксації доказів з відкритих. Як відомо, одним з критеріїв оцінки

допустимості доказів є також належне джерело. Відповідно, суб'єкт, який подає до суду докази, отримані з відкритих джерел, також має пояснити, звідки він дізнався або мав дізнатися про їх існування. Необхідно підкреслити, що така вимога на даний момент не є обов'язковою і, виходячи з аналізу судової практики, можна помітити, що суддям достатньо лише «кінцевого» доказу без вказівки «ланцюжка», який допоміг виявити такий доказ. Інколи сторона обвинувачення обмежується формулюванням «за допомогою інструментів OSINT було встановлено…» тощо, що також поки визнається як достатня аргументація. Власне таке та подібне формулювання також вказують на те, що отримання відомостей з відкритих джерел в деякій мірі прирівнюється до оперативно-розшукової діяльності. Так, в одному з вироків було зазначено наступне «… на виконання доручення слідчого у кримінальному провадженні … в порядку статті 41 КПК України, із застосування спеціалізованих засобів та сервісів «OPEN SOURCE INTELLIGENCE», проведено комплекс гласних оперативно-пошукових заходів спрямованих на встановлення ідентифікаційних властивостей засобу зв`язку НОМЕР_9 , якими користувалась потерпіла особа ОСОБА_5» [8].

В той же час також необхідно зважати на той факт, що чим частіше сторона обвинувачення буде використовувати докази, отримані з відкритих джерел, тим більше у сторони захисту буде з'являтися питань, та, відповідно, претензій, щодо порядку та специфіки їх отримання. Тому доцільно завчасно мінімузувати такі ризики.

В якості одного зі способів вирішення вказаної проблеми вчені пропонують складати не протокол оргляду окремого веб-сайту, а «протокол огляду з відкритих джерел мережі «Інтернет» [9], де має зазначатися поетапний опис послідовності дій під час огляду інформації з веб-сторінки. Власне вже можна побачити судові рішення, в яких сторона обвинувачення обмежується не лише оглядом однієї сторінки, а одразу надає алгоритм дій, які допомогли виявити відповідну інформацію, яка має значення для кримінального провадження: «Протоколом огляду від 16.03.2023 року, слідчим за участі спеціаліста, в період часу з 09-00 години до 11-10 години … зафіксовано огляд інформації, розміщеної у Всесвітній мережі

Інтернет стосовно відомостей щодо громадина РФ ОСОБА_8, ІНФОРМАЦІЯ_3. В ході огляду, використовуючи Інтернет браузер «Google Chrome» за електронною адресою посилання: https://www.google.com у полі пошуку головного меню було введено критерій пошуку «ОСОБА_8 (ІНФОРМАЦІЯ_22)». В процесі подальшого огляду було здійснено перехід на адресу посилання із заголовком …, що являє собою загальнодоступне інформаційне агенство «OBOZREVATEL» (ТОВ «Золота середина», поштова адреса: 01013, м. Київ, вул. Деревообробна, 7). Далі було здійснено огляд інформації, опублікованої 15.01.2023 року о 22:05 на вищезазначеній сторінці. В ході огляду розміщеної інформації встановлено, наступне…» [10]. Очевидно, що хоча в такий спосіб фіксація відомостей з відкритих джерел займає більше часу, проте мінімізує ризики того, що сторона кримінального провадження не зможе під час судового засідання пояснити, звідки вона взяла такі докази.

Також цікавою проблемою є необхідність дотримання правил користування відкритими джерелами, з яких отримується необхідна інформація. Якщо, наприклад, слідчій фіксує відомості зі сторінки в соціальній мережі, яка вимагає реєстрації, то слідчий сам має бути там зареєстрований. В той же час у всіх інструкціях та порадниках, які стосуються збирання відомостей з відкритих джерел, чітко зазначається, що особа, яка проводить OSINT розслідування, повинна в тому числі і перейматися власною безпекою, а тому не повинна використовувати свої справжні анкетні відомості. Відповідно, реєстрація в соціальній мережі під вигаданим іменем буде порушувати правила користування таким сервісом, що може вказувати на незаконний спосіб збирання доказів. В даному випадку можна зробити припущення, що доцільно буде використовувати «доктрину неминучого виявлення» («застосовується у тому випадку, якщо первинне джерело доказів було отримано у незаконний спосіб, водночас, такий доказ та похідні від нього докази приймаються до розгляду, якщо обвинувачення зможе довести, що оспорювана інформація «неминуче була б отримана законними методами» [11]), адже незалежно від облікового запису, яким би скористувався слідчий, такі докази все одно були б отримані.

Список використаних джерел:

1. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник / О. О. Торбас. Одеса : Видавництво «Юридика», 2024. 180 с.

2. Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. Судова влада України: веб-сайт. 07.06.2022. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/

3. Ухвала Костопільського районного суду Рівненської області від 26.06.2023, справа № 564/572/23. URL: https://reyestr.court.gov.ua/Review/111775060

4. Ухвала Святошинського районного суду м.Києва від 29.06.2023, справа № 759/11691/23. URL: https://reyestr.court.gov.ua/Review/111928130

5. Ухвала Павлоградського міськрайонного суду Дніпропетровської області від 19.06.2024, справа № 185/2082/24. URL: https://reyestr.court.gov.ua/Review/120171416

6. Ухвала Центрально-Міського районного суду міста Кривого Рогу Дніпропетровської області від 08.06.2022, справа № 216/1807/22. URL: https://reyestr.court.gov.ua/Review/104674268

7. Постанова ВС від 12.06.2024, справа № 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340

8. Вирок Великоолександрівського районного суду Херсонської області від 29.04.2024, справа № 650/1870/23. URL: https://reyestr.court.gov.ua/Review/118734665

9. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі): наук.-практ. порадник / Л.В. Гаврилюк, І.В. Басиста, Д.С. Афонін, А.В. Шевчишин та ін. Київ: ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с.

10. Вирок Жовтневого районного суду м. Запоріжжя від 04.04.2024, справа № 331/4290/23. URL: https://reyestr.court.gov.ua/Review/118116755

11. Доктрина заборони використання «плодів отруйного дерева» та винятки з неї: судова практика Великої Палати Верховного Суду в кримінальних провадженнях. Судова влада України: веб-сайт. 30.11.2020. URL: https://supreme.court.gov.ua/supreme/pres-centr/zmi/1031589/

БЄЛЯЄВ Євгеній Юрійович
асистент,
Національний юридичний університет
імені Ярослава Мудрого

КІБЕРЗАГРОЗИ, ЩО ВПЛИВАЮТЬ НА КРИТИЧНУ ІНФРАСТРУКТУРУ

На сьогодні кібератаки стають все більш частими, складними та шкідливими, критична інфраструктура стикається зі зростаючими ризиками в ключових секторах, таких як енергетика, фінанси, виробництво, охорона здоров'я, торгівля, урядові інформаційні системи, автоматизовані системи управління військами та зброєю тощо.

Поширення кіберзагроз викликає тривогу. Згідно з дослідженнями компанії Cybersecurity Ventures, яка займається вивченням глобальної кіберекономіки, у 2024 році кіберзлочинність обійдеться світу в 9,5 трильйонів доларів США [3]. Якщо вимірювати її як країну, то кіберзлочинність була б третьою за величиною економікою світу після США та Китаю.

Gartner, Inc – провідна світова дослідницька і консалтингова компанія у сфері інформаційних технологій, з головним офісом у Стемфорді, штат Коннектикут, США, прогнозує, що до 2025 року кіберзлочинці матимуть збройне середовище операційних технологій, щоб успішно завдавати шкоди або вбивати людей [4].

Передумовою для зростання кіберзагроз є той факт, що використання компонентів кіберзброї, як спеціальними службами іноземних держав, так і хакерами, злочинними або терористичними угрупуваннями, може забезпечити необхідний результат, що й при використанні класичних видів зброї. Для здійснення таких дій необхідні набагато менші витрати матеріальних та людських ресурсів, а також зменшується ризик викриття або отримання симетричної відповіді.

Важливо зазначити, що безпека критичної інфраструктури та підприємств складається з двох факторів: кібербезпеки та фізичної безпеки. Необхідно підкреслити, що ці фактори не можна розглядати окремо і що потрібен комплексний

кіберфізичний (CPS) підхід.

Абревіатура CPS розшифровується як Cyber-Physical Systems і відноситься до систем, які мають розподілену природу, складаються з фізичних елементів, які працюють у режимі реального часу та здатні спілкуватися один з одним за допомогою комунікаційної мережі (як дротової, так і бездротової). CPS об'єднує обчислювальні, комунікаційні та фізичні аспекти для покращення зручності використання, ефективності, надійності тощо. Однак такі комбінації створюють широкий спектр ризиків, наприклад, проблеми конфіденційності, кібератаки.

Кібербезпека об'єктів критичної інфраструктури і їх ланцюгів поставок має вирішальне значення з тієї простої причини, що ці системи живлять наше повсякденне життя – від електроенергії та води до охорони здоров'я та транспорту. Кібернетичний інцидент, який порушує роботу цих життєво важливих служб, може спричинити масовий хаос, поставити під загрозу життя, підірвати економіку та обороноздатність держави. Оскільки кіберзагрози стають дедалі складнішими та поширенішими, забезпечення стійкості та безпеки цих критично важливих систем є не просто технологічною необхідністю, а фундаментальною гарантією благополуччя та безперервності сучасного життя.

Запобіжні дії у сфері кібербезпеки є важливим аспектом, коли мова йде про кіберфізичні системи та її вплив на критичну інфраструктуру. Це вимагає виділення певної кількості ресурсів, однак це краще, ніж часто дороге відновлення (або, у гіршому випадку, відсутність відновлення взагалі). Насправді запобігання кіберінцидентам та кібератакам є тривалим і безперервним процесом, що виходить далеко за рамки технічних проблем, охоплюючи організаційні, нормативні та людські аспекти.

Згідно зі звітами [5, 6] Державної служби спеціального зв'язку та захисту інформації України про роботу Системи виявлення вразливостей та реагування на кіберінциденти та кібератаки за 2022 рік та 2023 рік, найбільша кількість атак була націлена на телекомунікаційний, урядовий, фінансовий, оборонний, а також енергетичний сектори України (таблиця 1).

Таблиця 1

Статистика моніторингу

Опис подій ІБ	2022р.	2023р.
Опрацьовано подій[1]	58 млрд	18 млрд
Детектовано підозрілих подій ІБ[2]	181 млн	133 млн
Опрацьовано критичних подій ІБ[3]	179 тис	148 тис
Зареєстровано кіберінцидентів[4]	415	1105

Примітки:

1 - отриманих за допомогою засобів моніторингу, аналізу та передання телеметричної інформації про кіберінциденти та кібератаки;

2 - при первинному аналізі;

3 - потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу;

4 - критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки;

Проведеним аналізом встановлено, що більшість кібератак здійснювалася з території рф, що свідчить про використання спецслужбами рф та підконтрольними їм хакерськими угрупуваннями вказаного інструменту для здійснення розвідувально-підривної діяльності проти України (блокування роботи телекомунікаційних систем та автоматизованих систем управління об’єктів критичної інфраструктури держави, з метою розміщення «фейкової» інформації, виведення з ладу обладнання об’єктів критичної інфраструктури або отримання віддаленого доступу до службової інформації з метою її несанкціонованого копіювання).

Ключові фактори кібератак на критичну інфраструктуру:

1. Поява Інтернету та мереж революціонізувала підключення та ефективність, але також забезпечила вектор для віддалених атак і крадіжки даних. З огляду на те, що виробничі та енергетичні об’єкти зараз під’єднані до Інтернету, цей вплив посилюється. Також величезна кількість підключених пристроїв і користувачів відкриває більше цілей.
2. Розвиток великих даних і хмарних сховищ також уможливив більше

потужних атак через накопичення конфіденційної інформації, як-от особистих медичних карток, фінансових даних і системних паролів. Пропонуючи централізований доступ і аналіз, ці величезні джерела дозволяють одиничним зломам скомпрометувати мільйони записів.

3. Зростаюча комерціалізація хакерства також сприяла нападам. Darknet сприяє злочинним діям, дозволяючи анонімно продавати вкрадені дані, зловмисне програмне забезпечення та послуги атаки. Геополітичний конфлікт є ще одним вектором загрози, коли спонсоровані державою групи намагаються зруйнувати інфраструктуру та викрасти інтелектуальну власність.
4. Застарілі системи та недостатня безпека на об’єктах критичної інфраструктури, використання застарілих систем керування. Складність сучасних мереж ускладнює виявлення вразливостей. Дефіцит фахівців з кібербезпеки загострює ці проблеми.

Типи загроз для критичної інфраструктури охоплюють від складного шкідливого програмного забезпечення та атак на ланцюги поставок до фізичних вторгнень і DDoS-атак. Хоча методи, які використовують зловмисники для порушення функціонування критичної інфраструктури, часто схожі на кіберзагрози загалом, їхній потенціал може спричинити широкомасштабні та тяжкі наслідки.

Враховуючи дуже взаємопов’язаний і взаємозалежний характер систем критичної інфраструктури, збій в одному секторі може мати каскадний вплив на інші. Наприклад, відключення електроенергії може вплинути на системи охорони здоров’я, зв’язку та транспорту. Крім того, враховуючи центральну роль критичної інфраструктури для функціонування країни, порушення роботи цих систем можуть мати значні наслідки для національної безпеки.

Необхідно зазначити, що при кібератаках на критичну інфраструктуру може бути порушена цілісність та конфіденційність інформації. Загрози такого роду можуть завдати шкоди суспільству аналогічним або навіть більш серйозним чином. Наприклад, витік особистих даних не можна скасувати, коли він стався, і це буде завдавати шкоди людям після інциденту.

Найпоширеніші загрози критичній інфраструктурі та основним службам включають:

1. Відмова в обслуговуванні та розподілені атаки. Кіберзагрози для критичної інфраструктури часто включають спроби порушити роботу служб через атаки на відмову в обслуговуванні, які призначені для переповнення серверу трафіком, що робить веб-сайт або онлайн-сервери критичної інфраструктури недоступними.

2. Таргетована кібератака або збій промислових систем управління. Кіберзагрози для критичної інфраструктури часто передбачають таргетовану кібератаку або збій систем промислового керування (ICS) і систем диспетчерського контролю та збору даних (SCADA), які використовуються для керування та автоматизації критичних процесів у таких секторах, як енергетика, водопостачання та виробництво.

3. Складне шкідливе програмне забезпечення. Кіберзагрози критичній інфраструктурі часто включають складне шкідливе програмне забезпечення та вдосконалені постійні загрози. Ці загрози розроблені таким чином, щоб залишатися непоміченими протягом тривалого часу, дозволяючи зловмисникам збирати розвідувальні дані, підвищувати привілеї та здійснювати скоординовані атаки зі значним ефектом.

4. Експлуатація вразливостей нульового дня. Уразливості нульового дня зазвичай збирають і використовують різні типи зловмисників. Ці вразливості є особливо серйозними, оскільки неможливо дізнатися, що вони використовуються, доки не станеться якийсь реальний вплив.

5. Соціальна інженерія. Соціальна інженерія відноситься до тактики, яка використовується для використання людської поведінки або помилки для отримання доступу до внутрішніх систем. Однією з найбільш поширених тактик є фішинг.

6. Фізичний доступ і гібридні атаки. Критична інфраструктура часто включає фізичні об’єкти, такі як електростанції, греблі та транспортні системи. Зловмисники можуть спробувати отримати фізичний доступ до цих об’єктів, безпосередньо або через внутрішні загрози, щоб скомпрометувати системи

зсередини. Вони можуть використовувати гібридні атаки, поєднуючи різні кібертехніки з фізичними діями.

7. Потрійне вимагання. Потрійне вимагання – це тактика, яку використовують зловмисники програм-вимагачів, де окрім крадіжки конфіденційних даних в організацій і погроз оприлюднити їх, якщо не буде здійснено платіж, вони також атакують клієнтів та/або ділових партнерів організацій і вимагають від них викуп.

8. Атаки на ланцюги поставок. Атака на критичні інфраструктури через ланцюг постачання програмного забезпечення є одним із кількох можливих векторів загрози, якими можуть скористатися зловмисники. Атаки на ланцюги поставок є зростаючою та все більш витонченою формою кіберзагрози. Вони націлені на складну мережу взаємовідносин між клієнтськими організаціями та їхніми постачальниками, постачальниками та сторонніми постачальниками послуг.

Механізми застосування цифрового захисту для критичної інфраструктури та основних послуг уже добре відомі. Окрім нових ризиків, які можуть виникнути з появою нових парадигм, таких як штучний інтелект або квантові обчислення, основні процеси безпеки можуть бути визначені в будь-якій стандартній структурі кібербезпеки, яку різні організації розробляли протягом останніх кількох десятиліть. Справжня складність виникає через неможливість захистити все заради простого питання ефективності (складні екосистеми неможливо захистити за допомогою простих процесів, оскільки вони потребують сегментації для цілеспрямованого захисту).

У відповідь на кіберзагрози як державний, так і приватний сектори економіки підвищують стійкість і відновлення, вживаючи комплексних заходів безпеки, включаючи підтримку надійної інвентаризації активів, розробку планів реагування на інциденти, впровадження надійних резервних копій даних, забезпечення оновлених систем з останніми виправленнями безпеки та нульовою архітектурою довіри, а також надійної політики ланцюга поставок. Тренінги з кібербезпеки також відіграють важливу роль, оскільки вони дають співробітникам необхідні знання щодо найкращих практик, спрямованих на створення надійної безпеки систем і

послуг із середини.

Список використаних джерел:

1. Про Стратегію кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни»: Указ Президента України від 26 серпня 2021 р.
№447/2021 / Президент України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 08.11.2024).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 р. №2163-VIII. / Верховна Рада Україна. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 08.11.2024).

3. Steve Morgan. Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024 / Cybersecurity Magazine. URL: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/#:~:text=A%20breakdown%20of%
20global%20cybercrime,%24182.5%20billion%20USD%20a%20week (дата звернення: 08.11.2024)

4. Susan Moore. Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans / Gartner. URL: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we (дата звернення 08.11.2024)

5. Звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератак за 2022 / ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ. URL: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit (дата звернення: 08.11.2024).

6. Звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератак за 2023 / ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ.

URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (дата звернення: 08.11.2024).

ДОБРОВОЛЬСЬКИЙ Марк Ігорович
студент,
Національний юридичний університет
імені Ярослава Мудрого

ЗАРУБІЖНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Інформаційна безпека сьогодні є не просто важливим аспектом державної політики, а й правовим поняттям, що отримало офіційне визнання. Під інформаційною безпекою розуміють стан, за якого забезпечено захист національних інтересів держави в інформаційній сфері, де інтереси особистості, суспільства та держави знаходяться в збалансованому співвідношенні. У наш час, коли світова інформаційна взаємодія досягла безпрецедентного рівня завдяки глобалізації, постає питання ослаблення інформаційного суверенітету держави. Інші країни та недержавні суб'єкти можуть впливати на внутрішню інформаційну політику через різноманітні канали – від інтернет-простору до медіа, що має значний вплив на безпеку будь-якої країни.

Інформаційна безпека стала одним із ключових пріоритетів сучасної міжнародної політики, адже її забезпечення вже не під силу окремим державам, навіть найпотужнішим. Однією з головних платформ для міжнародної взаємодії у сфері інформаційної безпеки є Організація Об'єднаних Націй (далі – ООН). Саме ООН, як організація з найбільш широким представництвом, може забезпечити комплексний підхід до вирішення глобальних інформаційних проблем, максимально враховуючи інтереси світової спільноти. Міждержавне співробітництво в цьому напрямі важливе не лише для протидії потенційним загрозам, а й для забезпечення

сталого розвитку інформаційної сфери в контексті збереження міжнародного миру та стабільності. Таке співробітництво включає розробку нових стандартів захисту, посилення координації між державами у випадках кіберзагроз та формування ефективної системи моніторингу й реагування на інформаційні атаки.

Ідея міжнародної інформаційної безпеки вперше отримала визнання на глобальному рівні з ухваленням Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» 4 грудня 1998 року, що стала першою офіційною спробою залучити міжнародну спільноту до обговорення створення спеціального міжнародно-правового режиму, який би регулював діяльність в інформаційній сфері. Основними структурними елементами майбутнього режиму визначалися інформація, інформаційні технології та способи їх застосування, що мало сприяти підвищенню глобальної безпеки. Наступним кроком стала Резолюція A/RES/54/49 від 1 грудня 1999 року, де вже чітко було зазначено, що інформаційний простір може бути джерелом загроз не лише для цивільної, а й для військової безпеки. У відповідь на цю резолюцію, у 2000 році Секретаріат ООН представив документ «Принципи, що стосуються міжнародної інформаційної безпеки», який виклав базові правила поведінки держав в інформаційному просторі, який став платформою для подальшого діалогу між державами та міжнародними організаціями під егідою ООН. Важливим аспектом розробки міжнародних документів у сфері інформаційної безпеки стало запровадження ключових термінів, що окреслили новий понятійний апарат. Такі терміни, як «інформаційний простір», «інформаційна безпека», «інформаційна війна» і «інформаційний тероризм», отримали своє офіційне визначення і заклали підґрунтя для формування подальшого міжнародного права в цій сфері. Запровадження таких термінів, як «інформаційна зброя», «неправомірне використання інформаційно-телекомунікаційних систем», «несанкціоноване втручання в інформаційні ресурси» та «критично важливі структури», продемонструвало глибокий розуміння того, наскільки вразливими можуть бути держави до кіберзагроз [1, с. 354].

Зокрема, важливі резолюції щодо боротьби зі злочинним використанням інформаційних технологій було ухвалено в 2000 та 2001 роках (A/RES/55/63 від 4 грудня 2000 р. і A/RES/56/121 від 19 грудня 2001 р.), вони заклали основи глобальної політики в боротьбі з кіберзлочинністю, приділяючи особливу увагу загрозам, що можуть порушити безпеку і стабільність країн, спільнот та окремих громадян. У 2002 році резолюція A/RES/57/239 ініціювала створення глобальної культури кібербезпеки, а наступні резолюції 2003 (A/RES/58/199) та 2009 років (A/RES/64/211) посилили акцент на захисті критичної інформаційної інфраструктури, яка стає все більш вразливою перед кібератаками, що можуть мати серйозні соціальні, економічні та навіть політичні наслідки. Одним із кроків у цьому напрямі стало ухвалення резолюції A/RES/62/17 від 5 грудня 2007 року, яка передбачала розгляд існуючих і потенційних загроз в інформаційній сфері на багатосторонньому рівні, сприяючи обміну досвідом і співпраці між країнами. Важливим здобутком у 2016 році стало ухвалення резолюції A/RES/71/28, в якій було визначено досягнення у сфері інформатизації та телекомунікацій, а також важливі кроки для забезпечення безпеки у контексті міжнародного миру та стабільності [2, с. 582].

Європейський Союз також активно працює у напрямі забезпечення інформаційної безпеки, надаючи цьому питанню пріоритетне значення в контексті розвитку своєї цифрової економіки. У 2001 році ЄС розробив перший масштабний документ – «Мережева та інформаційна безпека: європейський політичний підхід». Документ описував концептуальні основи мережевої безпеки, визначаючи її як здатність мереж і інформаційних систем протистояти випадковим подіям та зловмисним діям, що загрожують доступності, цілісності, конфіденційності та автентичності даних. Такий підхід наголошував на необхідності захисту інформації не лише від втрат чи крадіжок, але й від порушення її цілісності та доступності, що є ключовими елементами кібербезпеки. На додачу, у новій Стратегії кібербезпеки ЄС особлива увага приділяється захисту критично важливої інфраструктури, що підтримує функціонування таких секторів, як енергетика, фінанси, транспорт, охорона здоров’я тощо. ЄС намагається запроваджувати нові стандарти та регуляції,

що ускладнюють проникнення кібершахраїв до інформаційних систем та мінімізують ризики кібератак, що можуть паралізувати цілі галузі економіки [3, с. 166].

Європейський Союз вживає значних зусиль для забезпечення інформаційної безпеки, створюючи потужний організаційний механізм, здатний відповідати на виклики сучасного кіберпростору. Одним із головних елементів цієї системи є Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), засноване 10 березня 2004 року. Завданням ENISA є не лише вдосконалення мережевої та інформаційної безпеки на території ЄС, але й розвиток відповідної культури захисту даних і протидії кіберзагрозам. ENISA активно працює на благо громадян, бізнесу, громадських організацій та всіх учасників внутрішнього ринку ЄС, забезпечуючи безперервність його функціонування та захист інформаційного середовища від потенційних загроз. Крім організаційно-консультативної функції, ENISA сприяє впровадженню практичних заходів, таких як розробка нормативних стандартів кіберзахисту, проведення навчань з кібербезпеки та регулярні консультації з національними органами безпеки держав-членів, що дозволяє країнам ЄС ефективніше координувати свої дії у боротьбі з кібератаками та підвищувати рівень обізнаності громадян щодо кіберризиків.

Розуміючи, що глобальна кібербезпека неможлива без міжнародної співпраці, ЄС створив у структурі Європейського поліцейського офісу (Європол) Європейський центр боротьби з кіберзлочинністю (ЕС3) у 2013 році. Завдання цього Центру охоплюють розслідування кіберзлочинів, спрямованих на підрив критично важливої інфраструктури, захист інформаційних систем, а також протидію інтернет-шахрайству та іншим загрозам, що можуть порушувати стабільність кіберпростору ЄС. ЕС3 виконує роль аналітичного та оперативного центру, що не лише розслідує кіберзлочини, але й підтримує інформаційну взаємодію між державами-членами ЄС і зацікавленими міжнародними партнерами. Центр також забезпечує навчання та підвищення кваліфікації спеціалістів у галузі кіберзахисту, що дозволяє Європейському Союзу розвивати власні кадрові ресурси для протидії загрозам у цифровому середовищі [3, с.167].

У сучасному світі, де технології та інформаційні системи невпинно розвиваються, питання захисту критичної інфраструктури стає однією з найважливіших тем для національної безпеки багатьох країн. Під критичною інфраструктурою розуміють комплекс взаємопов'язаних систем, мереж і ресурсів, від стабільного функціонування яких залежить життя суспільства, зокрема безпека, економіка та добробут громадян. Об'єкти критичної інфраструктури забезпечують основні суспільні функції, включаючи енергопостачання, транспорт, медичне обслуговування, зв'язок, банківську діяльність і багато інших галузей, життєво важливих для сталого функціонування суспільства. Їхня особливість полягає також у тому, що вони можуть мати як цивільне, так і військове призначення або виконувати обидві функції одночасно. Забезпечення належного функціонування цих об'єктів є пріоритетом для держав, що підтверджується положеннями Резолюції Ради Безпеки ООН S/RES/2341 (2017) «Про захист критичної інфраструктури», ухваленої 13 лютого 2017 року [4, с. 282]. У ній зазначається, що кожна держава самостійно визначає, які саме об'єкти є критичними для її функціонування та повинні бути захищені на національному рівні.

Критичні об'єкти в різних країнах можуть мати різний статус та призначення. Наприклад, у США до них відносять не лише об'єкти, що забезпечують базові потреби суспільства, але й національні пам'ятки та історичні об'єкти, виборчу систему та дипломатичні місії. Такі об'єкти є потенційними мішенями для кіберзагроз, що зростають у сучасному інформаційному суспільстві, адже їхнє функціонування неможливе без цифрової інфраструктури та мереж, які підтримують системи управління, моніторингу та обробки даних. Взаємозалежність цих мереж сприяє обміну інформацією та оптимізації робочих процесів, однак водночас робить інфраструктуру вразливою до кібератак. З ростом можливостей віддаленого доступу до управління критичною інфраструктурою, з'являються нові виклики, пов'язані з кіберзагрозами. Доступність критичних систем через цифрові мережі значно підвищує ефективність їхнього обслуговування, проте відкриває нові можливості для кібератак з боку недружніх держав або злочинних угруповань. У наш час такі атаки часто набувають форми «кібервійни», що може мати руйнівні наслідки.

Приклади таких наслідків включають зупинку електростанцій, пошкодження нафтопроводів, переривання водопостачання, що призводить до дестабілізації функціонування всієї країни та підриває її національну безпеку.

Отже, інформаційна безпека у сучасному світі набуває комплексного значення: вона об'єднує держави у боротьбі з глобальними викликами і, водночас, забезпечує захист національних інтересів у межах кожної країни. Удосконалення міждержавного співробітництва у цій сфері є важливою передумовою для створення стабільного та безпечного інформаційного простору, здатного протистояти сучасним загрозам.

Список використаних джерел:

1. Кононенко В. П., Новікова Л. В. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. № 65. С. 353–358.
2. Сємко М. О. Нормотворча діяльність ООН щодо забезпечення інформаційної безпеки у воєнній сфері. *Юридичний науковий електронний журнал*. 2022. № 8. С. 580–583.
3. Фурсай О. Політика інформаційної безпеки Європейського Союзу. *Літопис Волині*. 2023. № 29. С. 165–170.
4. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО»*. 2020. № 29. С. 281–288.

КАЛИНЧУК Андрій В'ячеславович,
КОЛОБОВ Владислав Олександрович
студенти,
Національний юридичний університет
імені Ярослава Мудрого,
науковий керівник ***ЧЕРЕДНИЧЕНКО Олександр Юрійович***
професор, кандидат економічних наук, доцент,
Національний юридичний університет
імені Ярослава Мудрого

ОКРЕМІ АСПЕКТИ СПІВРОБІТНИЦТВА ДЕРЖАВИ УКРАЇНА З МІЖНАРОДНИМ КРИМІНАЛЬНИМ СУДОМ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ

Збройна агресія рф проти України, що почалася в 2014 році і набула широкомасштабного характеру у лютому 2022 року, поставила перед міжнародною спільнотою нагальне питання забезпечення правосуддя та притягнення винних до відповідальності за воєнні злочини, злочини проти людяності, а також злочин агресії. Одним із ключових інструментів у цьому процесі є співробітництво України з Міжнародним кримінальним судом (далі - МКС).

Співробітництво України з МКС базується на національному законодавстві, зокрема Законі України «Про співробітництво України з Міжнародним кримінальним судом» № 1129-IX від 19 лютого 2021 року. Закон визначає механізми взаємодії органів державної влади з Судом, включаючи надання доказів, забезпечення участі свідків і потерпілих, а також виконання запитів Суду [3].

Україна лише 21 серпня 2024 року ратифікувала Статут МКС та стала повноцінною учасницею цієї міжнародної установи[2]. Але, ще не будучи державою-учасницею Римського статуту МКС, відповідно до частини 3 статті 12 Статуту, Україна визнала юрисдикцію Суду шляхом подання декларацій у 2014 та 2015 роках [1], що дозволило МКС розпочати розслідування злочинів, вчинених на

території України, починаючи з 21 листопада 2013 року. Ратифікація Римського статуту для України, особливо в період повномасштабної війни, було непростим питанням, але ж дозволило покласти край чисельним дискусіям з приводу доцільності ратифікації Статуту МКС та поглибило співпрацю з Судом, що безумовно посилює міжнародно-правовий статус України.

У березні 2022 року Прокурор МКС Карім Хан ініціював розслідування щодо ситуації в Україні. Під час розслідування було задокументовано численні факти воєнних злочинів, включаючи навмисні атаки на цивільне населення, застосування забороненої зброї, насильницьке переміщення дітей та знищення культурних об'єктів [4]. Також, у березні 2023 року МКС видав ордери на арешт президента рф та уповноваженої з прав дитини за підозрою в депортації українських дітей [5]. Значну роль у збиранні доказів відіграють українські правоохоронні органи, міжнародні організації, а також громадянське суспільство. Наприклад, ініціатива «Україна. П'ята ранку» спрямована на документування воєнних злочинів і передачу доказів МКС [6].

Одним із основних викликів співробітництва є обмежена юрисдикція Суду щодо злочину агресії. Відповідно до статті 8-bis Римського статуту, МКС може розглядати справи щодо агресії лише у разі ратифікації Статуту як державою-агресором, так і державою-жертвою, що унеможливлює безпосередній розгляд злочину агресії рф проти України [1].

Іншою проблемою є забезпечення виконання ордерів на арешт. рф не визнає юрисдикцію МКС і не співпрацює з Судом, що ускладнює притягнення винних до відповідальності. Прикладом є ситуація, коли президент путін, попри ордер на арешт, продовжує брати участь у міжнародних заходах [5].

На нашу думку, для посилення ефективності співробітництва України з МКС необхідно вжити таких заходів:

- дозволити Україні брати активнішу участь у роботі Суду;
- ініціювати власні справи та зміцнити свою позицію на міжнародній арені;

- розширити національне законодавство шляхом внесення змін до Кримінального кодексу України з метою адаптації норм міжнародного кримінального права, включаючи злочини проти людяності та злочин агресії, що збільшить правову базу для притягнення винних до відповідальності на національному рівні;
- посилити міжнародний тиск на рф через спільні зусилля держав-учасниць МКС, міжнародних організацій та української дипломатії, спрямовані на більшу ізоляцію агресора та забезпечення виконання ордерів Суду;
- підтримати діяльність спеціального трибуналу щодо злочину агресії, оскільки ініціатива зі створення такого трибуналу для розслідування злочину агресії рф заслуговує на всебічну підтримку і може стати альтернативою для заповнення прогалин у юрисдикції МКС;
- активізувати розвиток технологій документування злочинів, зокрема використання цифрових технологій для збирання доказів, таких як геолокація, дрони, супутникові знімки, що сприятиме більш ефективному розслідуванню;
- систематичне та безперервне інформування суспільства про діяльність МКС через проведення просвітницьких заходів щодо важливості міжнародного правосуддя, які сприятимуть зміцненню довіри до Суду та забезпеченню підтримки з боку громадянського суспільства.

Громадянське суспільство України відіграє ключову роль у забезпеченні ефективної співпраці з Міжнародним кримінальним судом. Громадські організації, такі як «Центр громадянських свобод», ініціатива «Україна. П’ята ранку» та інші, активно займаються документуванням воєнних злочинів, збиранням доказів і формуванням баз даних. Наприклад, у 2023 році активісти ініціативи «Україна. П’ята ранку» передали до МКС докази насильницької депортації дітей з тимчасово окупованих територій, що стало одним із приводів для видачі ордерів на арешт представників керівництва РФ. Така взаємодія є важливим елементом забезпечення прозорості та об’єктивності розслідувань [6]. Окрім того, громадянське суспільство сприяє популяризації ідеї міжнародного правосуддя серед населення України.

Завдяки просвітницьким кампаніям, семінарам і тренінгам, які проводять громадські організації, дедалі більше українців усвідомлюють важливість співпраці з МКС і підтримують зусилля з притягнення агресора до відповідальності.

Співпраця України з МКС отримує значну підтримку з боку міжнародних партнерів. Зокрема, Європейський Союз і окремі держави, такі як Велика Британія, Канада та США, надають технічну, фінансову та експертну допомогу в документуванні злочинів і організації розслідувань. Програми міжнародного фінансування сприяють розвитку інфраструктури для зберігання доказів, створенню цифрових баз даних і підготовці слідчих. Однак виконання рішень МКС, зокрема ордерів на арешт, залишається викликом. Прикладом є складнощі, пов'язані з арештом вищого керівництва рф, оскільки вона не визнає юрисдикції Суду та ігнорує міжнародні зобов'язання. У цьому контексті важливою є координація міжнародних зусиль і впровадження додаткових санкцій проти осіб, які ухиляються від правосуддя. Залучення інших міжнародних судових органів і створення спеціальних механізмів, таких як трибунал щодо злочину агресії, можуть заповнити прогалини в юрисдикції МКС і сприяти справедливості.

Отже, співробітництво України з Міжнародним кримінальним судом є важливим елементом забезпечення правосуддя у контексті збройної агресії рф. Хоча цей процес стикається з численними викликами, він відкриває нові можливості для розвитку міжнародного кримінального права та посилення верховенства права. Ратифікація Римського статуту, підтримка спеціального трибуналу щодо злочину агресії, а також ефективна співпраця з міжнародними партнерами є ключовими напрямками, які дозволяють Україні досягти справедливості для жертв і притягнути винних до відповідальності.

Список використаних джерел:

1. Rome Statute of the International Criminal Court. URL: https://www.icc-cpi.int. (дата звернення: 25.11.2024).

2. Про ратифікацію Римського статуту Міжнародного кримінального суду та поправок до нього : Закон України від 21.08.2024 року №3909-20, Верховна Рада

України. URL: https://zakon.rada.gov.ua/laws/show/3909-20#Text (дата звернення: 25.11.2024).

3. Про внесення змін до Кримінального процесуального кодексу України та інших законодавчих актів України щодо співробітництва з Міжнародним кримінальним судом : Закон України від 03.05.2022 року №2236-20, Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2236-20#Text (дата звернення: 25.11.2024).

4. Office of the Prosecutor, International Criminal Court. Statement on the situation in Ukraine, 2022. URL: https://www.icc-cpi.int. (дата звернення: 25.11.2024).

5. International Criminal Court. Press Release: ICC issues arrest warrants in the context of the situation in Ukraine, March 2023. URL: https://www.icc-cpi.int.

6. Ukraine.5AM Coalition. URL: https://5am.org.ua. (дата звернення: 25.11.2024).

7. Проєкт спеціального трибуналу щодо злочину агресії. Офіційний сайт ООН. URL: https://www.un.org. (дата звернення: 25.11.2024).

КОГУТ Артем Анатолійович
старший викладач,
Національний юридичний університет
імені Ярослава Мудрого

НАДІЙНІСТЬ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

З розвитком Інтернету та комп'ютерних технологій в цілому піднялось на новий рівень питання захисту персональних даних. Так, мережа часів Web 1.0 вимагала захисту прав привілейованих користувачів для запобігання несанкціонованому доступу до зміни чи видаленню опублікованого контенту, але з трансформацією її у Web 2.0 та створенням соціальних мереж й інших інтерактивних сервісів, прив'язаних до ідентичності користувача, з'явилась велика

кількість різноманітних індивідуальних акаунтів та даних у них, які потребують захисту. Це – і облікові записи в соціальних мережах, і персональні кабінети на навчальних платформах, і корзини покупок в інтернет-магазинах. І крім зберігання персональних даних користувачів, багато з цих ресурсів мають доступ до платіжних інструментів та можливість вчинення від імені конкретної особи різноманітних дій, починаючи від листування, закінчуючи купівлями тощо.

В розвитку мережевих інструментів Україна пішла далі, ніж більшість держав світу. Вона не тільки розвинула можливість мобільного вчинення банківських транзакцій, але ще й впровадила реалізацію цивільної правосуб'єктності онлайн. Це включає в себе широкий перелік дій, що вчиняються з використанням комп'ютерів (в т.ч. мобільних пристроїв), починаючи від ідентифікації особи, відкриття рахунків, оформлення матеріальної допомоги, реєстрації народження дитини, закінчуючи укладенням шлюбів та купівлею-продажем транспортних засобів.

Раніше основним способом захисту даних та підтвердження належного користувача був пароль, і для його захисту використовувались різні інструкції: належне зберігання, відмінність від імені користувача, достатня складність (що враховувала, наприклад, мінімальну довжину, наявність літер з обох регістрів, цифр та спеціальних символів), відсутність словарних слів тощо. При цьому, зловмисниками використовувався широкий інструментарій їх зламу: від соціальної інженерії до банального перебору «грубою силою». А з появою в мережі зазначених вище дуже чутливих даних, простих паролів стало замало для надійного їх зберігання, і на допомогу прийшла авторизація за допомогою токенів (фізичних ключів, призначених для ідентифікації його власника) та двофакторна автентифікація, яка передбачає після введення звичайного паролю, підтвердження «другим фактором» - кодом, отриманим від окремої програми на мобільному пристрої чи комп'ютері. При цьому, вказаний код може передаватись і засобами електронної пошти на довірену адресу, і повідомленням на визначений раніше номер телефону. Більш розвиненим та новим способом двофакторної автентифікації є використання біометричних даних користувача (як то усім відомий «квест» - «покліпати очима в додаток «ДіЯ»). Але він є досить дорогим в реалізації, і для

менш чутливих даних оптимальним для розробників лишається підтвердження через пошту чи СМС-повідомлення.

І якщо у багатьох користувачів, що дотримуються базових правил кібергігієни, можуть бути сумніви щодо надійності електронної пошти через можливість компрометування паролю та отримання доступу до скриньки сторонніми особами, то до повідомлення з мобільного телефону на перший погляд питань з боку надійності не виникає.

Але це все не зовсім так. Передусім, телефон не завжди знаходиться у полі зору власника. І «умовно близька» особа може скористатись моментом для запиту паролю підтвердження до певного ресурсу. Тут виходом є базові правила щодо блокування телефону та заборони висвітлення тексту повідомлень на замкненому екрані (при чому, як і отриманих за допомогою СМС, так і повідомлень з месенджерів, оскільки зараз багато розробників з метою здешевлення процедури використовують їх для надсилання кодів підтвердження). При чому, сам обліковий запис в месенджері теж може бути «розповсюджений» на сторонні пристрої, що теж ставить під загрозу двофакторну автентифікацію. Другим, і більшим ризиком, від якого складніше вберегтися, є можливість «крадіжки» номеру, що у випадку з фінансовим номером надає зловмисникам майже повне володіння ідентичністю користувача в мережі.

Найпростішим способом вчинення такої крадіжки є фізичний перевипуск сторонньою особою сім-карти (е-сім) жертви. З метою убезпечення від цього оператори мобільних послуг мають алгоритми захисту, але вони є недосконалими і достатньо легко обходяться. Так, основними з них є подання оператору інформації щодо останніх вчинених з номеру телефонних дзвінків та відомостей щодо дати та суми поповнення рахунку.

Список телефонних дзвінків отримується різноманітними інструментами соціальної інженерії, коли жертву протягом короткого часу «провокують» перетелефонувати на визначені номери: до банківських операторів, в різні сервіси, організаторам лотерей тощо (залежно від особистісних рис жертви). З поповненням рахунку все набагато простіше: невстановлена особа поповнює мобільний рахунок

жертви у певний час на конкретну суму. Наявність подібних ситуації повинно слугувати для особи «червоним прапором», що її номер намагаються викрасти. І якщо з вихідними дзвінками все достатньо просто – необхідно бути пильним та уникати такого роду провокувань, то щодо поповнення мобільного номеру – у користувача немає дієвих алгоритмів уникнення.

Разом з тим, зазвичай оператори мають можливість застосування додаткових засобів безпеки: наприклад, заборона заміни сім-карти без фізичної присутності абонента в приміщенні оператора зв'язку або ж перехід на контрактну форму обслуговування, що хоч і створює певні незручності користувачу (у випадку відновлення втраченої сім-карти), але є надійним механізмом захисту номеру.

Враховуючи викладене, необхідно мати на увазі, що прогрес у сфері інформаційних технологій щодня дає нам додаткові зручності і блага, але поруч з ним йде і кіберзлочинність, яка експлуатує ці зручності при реалізації злочинних задумів. У зв'язку з цим, обсяг процедур, що передбачає користувацька кібергігієна, щоденно збільшується, і, якщо ще не так давно достатньо було мати пароль, відмінний від «qwerty» чи «password», то зараз необхідний мінімум у рази вищий.

КОЛЕСНИКОВ Максим Євгенович
студент,
Національний юридичний університет
імені Ярослава Мудрого

СУЧАСНІ МЕТОДИ ЗБОРУ ЦИФРОВОЇ ІНФОРМАЦІЇ ТА ОСОБЛИВОСТІ ЇЇ ВИКОРИСТАННЯ ПІД ЧАС ДОКАЗУВАННЯ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

У сучасному інформаційному суспільстві зростає кількість користувачів різних цифрових пристроїв, автоматизованих мереж і систем, які створюють, обробляють, передають та зберігають дані, охоплюючи всі сфери суспільних

відносин. Цифрові докази, як новий вид кримінальних доказів на основі дискретних даних, виникли через стрімку комп'ютеризацію та збільшення правових відносин в інформаційному просторі. Їх використання стає надзвичайно важливим для захисту державної безпеки, зокрема підрозділами Служби безпеки України [1, 3].

Застосування цифрової інформації для формування доказів у кримінальному процесі з часом набуло ознак усталеної практики, оскільки в сучасному суспільстві вона є одним із найпоширеніших джерел даних про людей і події. Сьогодні цифрові докази іноді є вирішальними для встановлення фактів та обставин можливих кримінальних правопорушень, які відбулися в суспільстві. Це зумовлено зростанням кількості злочинів, що здійснюються з використанням цифрових технологій, електронних комунікаційних мереж, шкідливого програмного забезпечення та методів соціальної інженерії для отримання персональних ідентифікаційних даних. Практика показує, що цифрові докази, отримані під час проведення негласних слідчих розслідувань, дозволяють отримати достовірну інформацію не лише про осіб, причетних до злочину, але й про потенційних свідків, потерпілих, місця зберігання знарядь злочину, предмети та документи, що містять дані про перебіг злочинних дій, а також невстановлені зв'язки підозрюваних осіб. За допомогою цифрових слідів часто вдається встановити осіб, які зникли безвісти, місця приховування розшукуваних, їх озброєння та іншу інформацію, яка може сприяти або, навпаки, ускладнювати процес затримання [2, 3, 4].

Цифрові докази мають певні особливості, які істотно відрізняють їх від будь-яких інших видів доказів. На рис. 1 відображено певні характерні особливості.

Рис. 1 Характерні особливості цифрових доказів

На практиці цифрові докази класифікуються або як речові докази (наприклад, жорсткі диски чи оперативна пам’ять, на яких може зберігатися значуща цифрова інформація), або як документи (матеріали цифрової фотозйомки, звукозаписів, відеозаписів тощо) [4].

На сьогодні існує досить велика кількість способів отримання (вилучення) та безпосереднього використання цифрової інформації, що є корисною для правоохоронних органів під час доказування у кримінальному процесі в якості безпосередніх доказів. На рис. 2 зазначені найбільш вагомі з них.

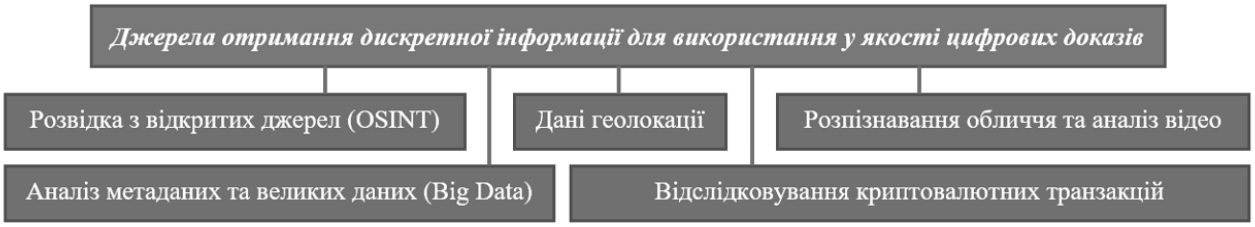

Рис. 2 Джерела отримання дискретної (цифрової) інформації для використання її у якості цифрових доказів правоохоронними органами

Так, одним з найпоширеніших є **розвідка з відкритих джерел**. **OSINT (open-source intelligence)** – це процес збору та аналізу інформації, отриманої з публічно доступних ресурсів, а також з таємних джерел і загальнодоступних даних (PAI – publicly available information), з метою отримання розвідувальної інформації, яка може бути використана на практиці. Це може бути застосовано правоохоронними органами як у сферах національної безпеки, так і цивільними особами, наприклад, у бізнес-розвідці. На рис. 3 зазначені категорії джерел OSINT **[6].**

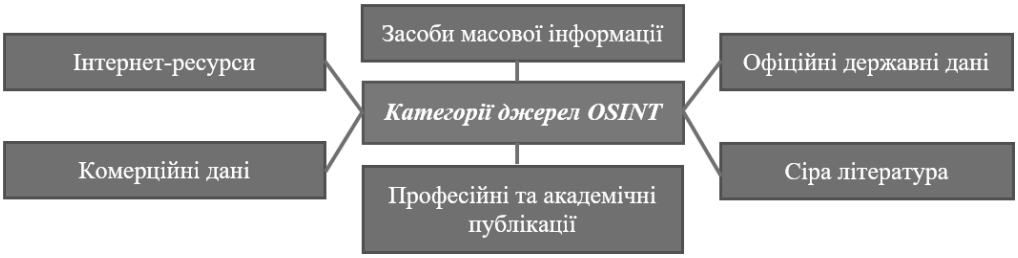

Рис. 3 Категорії джерел OSINT, через які здійснюється збір необхідної інформації

Сьогодні **розвідка з відкритих джерел є невід’ємною частиною війни. Кожного дня співробітники Служби безпеки України отримують купу цінної інформації про ворога шляхом використання цього методу. Крім цього залучаються і небайдужі громадяни, які сприяють процесу пошуку необхідних**

даних, які «оновлюються» ворогом під час необачних його дій, наприклад, у соц-мережах.

Наступним та не менш важливим є використання даних геолокації. Насамперед, геолокація – це **визначення фактичного географічного місцезнаходження електронного пристрою**, такого як радіопередавач, мобільний телефон або комп'ютер, який має підключення до Інтернету [7].

Дані геолокації можуть підтвердити або спростувати місцезнаходження підозрюваних у певний час, що є важливим для встановлення їхньої участі у злочині. Аналіз переміщень допомагає відновити маршрути підозрюваних, виявити зв'язки між різними місцями подій та визначити потенційні точки зіткнення. Ці дані можуть бути використані для підтвердження або спростування алібі підозрюваного, що є важливим доказом у судовому процесі.

Особливого значення геолокація набуває в умовах війни, де відстеження ворога за визначенням його місця розташування через мобільні пристрої або інші гаджети, що мають GPS-модуль дозволяє ефективно виконувати поставлені задачі. Визначення геопозиції є одним з найприорітетніших завдань Служби безпеки України у боротьбі із супротивником.

Наступним є технології розпізнавання обличчя та аналіз відео. Перше є видом біометричної технології, яка дозволяє користувачам швидко ідентифікувати осіб, що з'являються у відеозаписах. За допомогою спеціального програмного забезпечення відбувається процес ідентифікації осіб на основі їхніх біометричних характеристик, таких як форма обличчя, розташування очей, носа та інших унікальних ознак [8].

Аналіз відео передбачає обробку та інтерпретацію відеозаписів для виявлення підозрілої діяльності. Так, вже найбільш поширеним є використання цієї технології у камерах дорожнього руху (рис. 4).

Рис. 4 Технологія розпізнавання об'єктів у дорожньому русі [9]

Це може охоплювати відстеження руху осіб, виявлення аномальної поведінки, визначення часу та місця перебування підозрюваних, а також інші важливі деталі, які можуть бути використані у судовому процесі. **Так, наприклад, системи відеоспостереження**, що оснащені алгоритмами розпізнавання обличчя, дозволяють автоматично ідентифікувати осіб. Це значно полегшує роботу правоохоронних органів у пошуку та ідентифікації підозрюваних, особливо в умовах великого скупчення людей або на масових заходах. Такі технології дозволяють як ідентифікувати підозрюваних, так і відстежувати їхні переміщення, визначати взаємозв'язки між різними особами та встановлювати час та місце перебування підозрюваних під час вчинення злочину.

Метадані та великі дані (Big Data) є ключовими компонентами, які використовуються у сучасних кримінальних процесах, особливо у справах, пов'язаних із національною безпекою. Ці методи дозволяють ефективно обробляти та інтерпретувати великі обсяги інформації для виявлення прихованих зв'язків, аналізу тенденцій та прогнозування потенційних загроз. Вони охоплюють обробку та аналіз величезних обсягів різнорідної інформації з використанням передових алгоритмів машинного навчання та штучного інтелекту. Завдяки цьому, правоохоронні органи можуть ефективно виявляти складні «патерни» поведінки,

встановлювати взаємозв'язки між різними суб'єктами та подіями, а також прогнозувати можливі загрози на основі аналізу великих масивів даних.

Цей метод має і практичне значення. Наприклад, його використання може допомогти під час розслідування мережі фінансових злочинів, де аналіз дозволяє виявити незвичайні фінансові транзакції, які можуть свідчити про відмивання грошей. Такий підхід допомагає значно скоротити об'єм роботи співробітників правоохоронних органів, а також підвищити їх оперативність та ефективність дій.

Ще одним значним аспектом використання цифрової інформації під час кримінального процесу є відслідковування криптовалютних транзакцій. Криптовалютні злочини охоплюють широкий спектр незаконних дій, пов'язаних із використанням криптовалют та блокчейн-технологій. З розвитком цифрових фінансів виникли нові можливості для здійснення фінансових злочинів, таких як відмивання грошей, підтримки терористичних угруповань (наприклад, фінансування колаборціоністів в умовах війни), шахрайство, торгівля нелегальними товарами та інші протиправні дії. Аналіз криптовалютних злочинів стає критично важливим для забезпечення національної безпеки, оскільки криптовалюту часто використовують для анонімних транзакцій, що ускладнює їхнє відстеження та розслідування. Проте, незважаючи на зростаючу важливість цифрової валюти в Україні, незаконний її обіг все ще не регулюється належним чином, залишаючи вільне місце для протиправних дій правопорушників.

Отже, підсумовуючи можна визначити, що у сучасному інформаційному суспільстві цифрова інформація стала невід'ємною складовою багатьох сфер діяльності, включаючи правоохоронну та судову системи. Використання цифрової інформації під час доказування у кримінальному процесі по злочинам проти основ національної безпеки набуває особливого значення, оскільки такі злочини часто пов'язані з використанням передових технологій та потребують відповідних методів розслідування. Такі особливості вимагають від правоохоронних органів нових підходів до збору, аналізу та збереження доказової бази. Зазначені методи (джерела) отримання та подальшого використання отриманої інформації дозволяють:

- Ефективно збирати інформацію про підозрюваних та їхню діяльність;

- встановлювати місцезнаходження та переміщення осіб, пов’язаних зі злочином;
- виявляти зв’язки між учасниками протиправних дій;
- прогнозувати та запобігати потенційним загрозам на основі аналізу отриманих даних.

Сучасні аспекти використання цифрової інформації у кримінальному процесі є критично важливими для здійснення ефективних дій з боку правоохоронних органів. Завдяки інтеграції передових технологій є змога ефективно забезпечувати національну безпеку та захищати права громадян. Тепер цифрові докази є невід’ємною частиною нашого буття.

Список використаних джерел:

1. Kessler G. Judge’s Awareness, Understanding, and Application of Digital Evidence. Miami: Nova Southeastern University, 2010. 182 с. (дата звернення 06.11.2024)

2. Метелев О. П., Коваленко Є. В. До питання використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно-розшукової діяльності // Науковий вісник Ужгородського Національного Університету. 2023. Вип. 80(2). С. 177–182. DOI: https://doi.org/10.24144/2307-3322.2023.80.2.27 (дата звернення 06.11.2024)

3. Метелев О. П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження // Науковий вісник Ужгородського національного університету. 2020. Вип. 60. С. 177–180. DOI: https://doi.org/10.32782/2307-3322/2020.60.39 (дата звернення 07.11.2024)

4. Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика // Вісник кримінального судочинства. 2023. № 1–2. С. 42–53. DOI: https://doi.org/10.17721/2413-5372.2023.1-2/42-53 (дата звернення 08.11.2024)

5. Кряковцев С. М. Дотримання особистих прав людини в процесі зняття інформації з транспортних телекомунікаційних мереж // Вісник Луганського

державного університету внутрішніх справ імені Е.О. Дідоренка. Сєвєродонецьк, 2014. Вип. 2. С. 291–299. (дата звернення 08.11.2024)

6. Макс Зосим. Розвідка з відкритих джерел (OSINT) [Електронний ресурс]. URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ (дата звернення: 09.11.2024)

7. Geopositioning [Електронний ресурс] / Wikipedia. URL: https://en.wikipedia.org/wiki/Geopositioning (дата звернення: 09.11.2024).

8. Особливості вибору технологій розпізнавання облич для організацій [Електронний ресурс] / World Vision Ukraine. URL: https://worldvision.com.ua/osobennosti-vybora-tekhnologii-raspoznavaniya-lits-dlya-organizatsiy/ (дата звернення: 09.11.2024).

9. Feurer M., Klein A., Eggensperger K., Springenberg J.T., Blum M., Hutter F. Auto-sklearn: Efficient and Robust Automated Machine Learning. *PeerJ Computer Science*. 2020 DOI: https://doi.org/10.7717/peerj-cs.586/

КОЛІСНИЧЕНКО Владислав Олегович

студент,

Національний юридичний університет

імені Ярослава Мудрого

АКТУАЛЬНІ КІБЕРЗАГРОЗИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: ВИДИ АТАК ТА СПОСОБИ ЗАХИСТУ

У наш час важливість кібергігієни важко переоцінити. Кожен користувач Інтернету має базову відповідальність за захист своїх особистих даних і пристроїв від кіберзагроз. Кібергігієна включає в себе набір простих, але ефективних заходів, які дозволяють зменшити ризики та уникнути небажаних наслідків. Одним із основних кроків є регулярне оновлення програмного забезпечення. Багато атак відбувається через вразливості, які були виявлені ще до того, як їх виправили

розробники. Оновлення операційних систем, програм-антивірусів та інших додатків можуть виправити ці вразливості, знижуючи ймовірність атак на пристрій користувача. Також важливим аспектом є створення складних паролів. Паролі повинні містити різні типи символів — великі й малі літери, цифри, спеціальні знаки. Це значно ускладнює їх підбір навіть за допомогою програм для брутфорсу. Крім того, наявність двофакторної автентифікації може значно підвищити безпеку облікових записів, оскільки для доступу до акаунтів необхідно підтвердити особу не лише за допомогою пароля, а й додатково, через код, надісланий на мобільний телефон або електронну пошту.

Але навіть якщо ви дотримуєтесь основ кібергігієни, це не гарантує повного захисту. Загрози в Інтернеті стають дедалі складнішими, і зловмисники постійно знаходять нові способи обходити існуючі захисні системи. Однією з найбільших загроз є крадіжка персональних даних. Це можуть бути не лише фінансові дані, такі як номери кредитних карток, але й особисті відомості, адреси, телефони, що можуть бути використані для здійснення шахрайських дій. Для цього зловмисники часто використовують фішинг-атаки — підроблені листи або вебсайти, які виглядають як офіційні джерела, з метою змусити користувачів ввести свої особисті дані. Важливо завжди перевіряти правильність адреси сайту або джерела листа, оскільки фішингові атаки часто маскуються під перевірені та відомі платформи.

Іншими небезпеками є віруси, трояни, програми-вимагачі та інші види шкідливого програмного забезпечення, які можуть потрапити на комп'ютери через небезпечні посилання або заражені файли. Ці програми здатні красти дані, блокувати доступ до важливих файлів або навіть шифрувати їх, вимагаючи викуп за відновлення доступу. Щоб уникнути цього, необхідно не лише регулярно оновлювати антивірусне програмне забезпечення, а й уважно ставитись до того, які файли ви завантажуєте або відкриваєте на своєму пристрої.

Захист анонімності в Інтернеті є ще одним важливим аспектом безпеки. Користувачі часто недооцінюють, яку кількість особистої інформації можна отримати просто з даних про місцезнаходження, IP-адреси чи інші параметри. За допомогою різних технологій можна відстежувати діяльність користувачів, що може

порушити їх право на приватність. Для захисту приватних даних багато користувачів використовують VPN (віртуальну приватну мережу), яка шифрує Інтернет-з'єднання і дозволяє анонімно серфити по Інтернету, приховуючи реальний IP-адрес. VPN створює захищений тунель для даних, який ускладнює доступ до них зловмисників. Окрім того, популярним інструментом для забезпечення анонімності є мережа Tor, яка дозволяє серфити в Інтернеті, приховуючи не лише IP-адресу користувача, а й шифруючи весь трафік. Проте, незважаючи на високий рівень захисту, навіть ці інструменти не є абсолютно безпечними, оскільки існують технології, які дозволяють зібрати інформацію про користувача, навіть якщо він використовує VPN або Tor. Це може бути зроблено через використання трекерів, таких як cookies або browser fingerprinting — унікальних характеристик браузера, які можна використовувати для відстеження користувачів.

Персональні дані — це одна з найбільших цінностей у цифровому світі, тому їх захист є пріоритетом для кожного користувача Інтернету. Шифрування є найефективнішим методом захисту даних. Зашифровані повідомлення та транзакції стають недоступними для сторонніх осіб, навіть якщо дані потрапляють у чужі руки. Так, наприклад, більшість популярних месенджерів, таких як WhatsApp або Telegram, використовують шифрування для захисту особистих повідомлень. Шифрування також використовується для захисту даних під час фінансових операцій. Якщо ви використовуєте електронний банкінг або здійснюєте онлайн-покупки, переконайтеся, що сайт має захищене з'єднання (це можна визначити за наявністю "https" в адресному рядку та значком замка).

Захист персональних даних також регулюється законодавством. Одним із найбільш відомих законів є GDPR (General Data Protection Regulation) в Європейському Союзі, який дає користувачам право на доступ, зміну чи видалення своїх персональних даних. Це законодавство також вимагає від організацій вжиття заходів для забезпечення захисту даних. Для цього використовуються різні методи шифрування, безпечні канали передачі даних та інші інструменти, що дозволяють уникнути витоків інформації. Важливою складовою захисту персональних даних є також підвищення обізнаності користувачів, оскільки більшість порушень безпеки

стаються через людський фактор, коли користувачі випадково розкривають свої дані через незахищені канали.

Крім того, важливо розуміти роль освіти в кібербезпеці. Люди, які не знають про основи захисту в Інтернеті, частіше стають жертвами кіберзлочинців. Підвищення обізнаності серед громадськості допомагає знизити ризики. Важливо вчити користувачів розпізнавати фішингові атаки, створювати надійні паролі і користуватися двофакторною автентифікацією, а також навчати базовим принципам безпеки в Інтернеті.

Важливо також зазначити, що хоча анонімність в Інтернеті є правом кожного користувача, вона може бути використана й для незаконних цілей, таких як кіберзлочинність. Зловмисники можуть використовувати анонімні мережі для здійснення атак чи організації інших незаконних дій. Тому вкрай важливо знайти баланс між правом на приватність і необхідністю боротьби з кіберзлочинністю.

Список використаних джерел:

1. Шнайдер Б. Кібербезпека: Стратегія і практика. Wiley, 2021.
2. Безпека даних. *ESET*. URL: https://www.eset.com/ua/.
3. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України".
4. Кеннеді М. Інтернет-безпека: від основ до практики. DeGruyter, 2020.

ЛЕВИЦЬКИЙ Антон Павлович
студент,
Національний юридичний університет
імені Ярослава Мудрого

РОЛЬ ЦИФРОВІЗАЦІЇ У ЗАБЕЗПЕЧЕННІ ПРАВ ЛЮДИНИ ПІД ЧАС ВОЄННОГО СТАНУ: АНАЛІЗ ЗАКОНОДАВЧИХ ПІДХОДІВ ТА ПРАКТИЧНИХ РІШЕНЬ

Цифровізація є рушійною силою змін у суспільстві, впливаючи на взаємодію держави і громадян, зокрема на реалізацію та захист прав людини. Під час воєнного стану цифрові технології стають особливо важливими, оскільки вони допомагають забезпечити доступ до інформації, державних послуг, правової допомоги, соціальних виплат, гуманітарної підтримки та захисту персональних даних. Тема цифровізації прав людини є надзвичайно актуальною, оскільки правові та технологічні новації у цій сфері забезпечують механізми для реалізації базових прав та потреб громадян у надзвичайних умовах.

У сучасних умовах війни цифровізація потребує адаптованої законодавчої бази, яка відповідає потребам громадян і вимогам безпеки. Законодавчі акти, що регулюють цифрові права, повинні забезпечувати баланс між захистом прав людини і безпекою держави.

Постановою Кабінету Міністрів від 18 вересня 2019 року № 856 було затверджено Положення про Міністерство цифрової трансформації України, яке визначає основні засади діяльності, повноваження та компетенцію цього нового органу. З метою виконання ключових завдань, покладених на Міністерство як головний орган центральної виконавчої влади у сфері цифрового розвитку та інновацій, був розроблений та презентований проект «Цифрова держава», що є найбільшим цифровим проектом в сучасній Україні.

4 грудня 2019 року Кабінет Міністрів України затвердив Положення про Єдиний державний веб-портал електронних послуг, визначивши його мету,

завдання, склад учасників (користувачів, включаючи суб'єкта звернення та суб'єкта розгляду звернень, держателя та технічного адміністратора) та функціональні можливості порталу «Дія». Міністерство цифрової трансформації анонсувало плани щодо забезпечення технічних можливостей для доступу до

100 % державних послуг через портал та мобільний додаток «Дія». В умовах війни електронні документи значно полегшують доступ громадян до державних послуг і підтвердження особи. Впровадження електронних документів є важливою частиною цифровізації прав людини, оскільки воно дозволяє громадянам ідентифікувати себе навіть у зонах обмеженого доступу до державних установ. Прикладом цього є данний застосунок, який став важливим інструментом для українських громадян під час війни.

В умовах кіберзагроз, пов’язаних з воєнним станом, захист персональної інформації набуває особливого значення. Закони про кібербезпеку і захист даних мають на меті не лише захистити дані громадян, а й запобігти витоку інформації, що може бути використана проти держави. Удосконалення правових норм щодо захисту персональних даних знижує ризик несанкціонованого доступу та зловживання даними.

Законодавство, яке регулює доступ до правової інформації, є ключовим для захисту прав людини під час війни. Створення законодавчих актів, що підтримують дистанційний доступ до правової допомоги через онлайн-платформи, дозволяє громадянам вирішувати питання, пов'язані з соціальними виплатами, переміщенням, гуманітарною допомогою та іншим.

Поряд із законодавчими аспектами, практичні рішення є основним інструментом для реалізації прав людини під час війни. Ось основні напрями таких рішень, що можуть бути досліджені:

Умови війни часто обмежують фізичний доступ до державних установ. Електронні документи та цифрові ідентифікаційні системи дозволяють громадянам підтвердити свою особу у віддалених умовах. Це особливо важливо для переселенців, які можуть потребувати документів для отримання допомоги або доступу до державних послуг у нових місцях проживання.

Онлайн-сервіси дозволяють отримати консультації щодо соціальних виплат, правових питань, гуманітарної допомоги тощо. Такі платформи працюють за принципом "єдиного вікна," де користувачі можуть отримати консультації від юристів, психологів, соціальних працівників. Наприклад, гарячі лінії та онлайн-консультації, доступні на державних сайтах, допомагають громадянам швидко отримати необхідну допомогу.

У період війни створюються спеціальні платформи для обліку гуманітарної допомоги, переміщених осіб та їхніх потреб. Вони дозволяють моніторити потреби населення і забезпечувати координацію постачання гуманітарної допомоги в реальному часі.

Використання цифрових інструментів дозволяє фіксувати випадки порушення прав людини і забезпечувати збереження доказів для можливих розслідувань. Наприклад, спеціальні платформи та мобільні додатки можуть бути використані громадянами для інформування про порушення прав, що забезпечує прозорість і підзвітність.

Під час війни зростає потреба у знаннях про кібербезпеку, захист персональних даних і основні права людини в цифровому середовищі. Освітні програми з цифрової грамотності допомагають громадянам розуміти, як захистити свої дані, уникати онлайн-шахрайства і безпечно використовувати державні онлайн-сервіси. Такі програми можуть реалізовуватись через соціальні медіа, вебінари, онлайн-курси тощо.

У відповідь на зростання кіберзагроз, держава повинна впроваджувати нові протоколи безпеки, щоб зберегти недоторканність персональних даних. Такі заходи включають посилення захисту баз даних, шифрування інформації та підвищення кіберграмотності державних службовців.

Цифровізація є важливим інструментом для захисту прав людини під час воєнного стану. Завдяки електронним документам, онлайн-платформам для правової та соціальної допомоги, системам моніторингу правопорушень і освітнім програмам, громадяни отримують доступ до базових послуг та інформації навіть у кризових умовах. Законодавчі зміни у сфері цифровізації сприяють посиленню

захисту прав людини, забезпечуючи сталість державних функцій та підтримку громадян у складні часи.

Список використаних джерел:

1. Положення про Міністерство цифрової трансформації України : Постанова Кабінету Міністрів України від 18.09.2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF

2. Про затвердження Указу Президента України «Про введення воєнного стану в Україні» : Закон України від 24.02.2022 р. № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/2102-20

3. Офіс Президента України. "Дія як цифровий паспорт: перспективи використання мобільного додатка під час воєнного стану". Офіційний вебсайт Офісу Президента України, 2023 р. Доступ: https://president.gov.ua.

4. Швець, О. С. "Роль цифровізації в умовах воєнного стану: український досвід". Збірник наукових праць з прав людини, 2023 р.

ЛЕОНОВИЧ Михайло Юрійович

студент,

Національний юридичний університет

імені Ярослава Мудрого

Науковий керівник: ***Олексій МЕТЕЛЕВ,***

доктор філософії у галузі права, завідувач кафедри,

Національний юридичний університет

імені Ярослава Мудрого

КІБЕРТЕРОРИЗМ: ЗАГРОЗИ ТА ВИКЛИКИ

Кібертероризм є однією з найбільших загроз сучасності. Стрімкий розвиток інформаційних технологій та широке використання Інтернету та комп'ютерних

систем у всіх сферах життя суспільства створюють нові можливості для правопорушень. Кібертерористи можуть завдавати величезної шкоди економіці, інфраструктурі та навіть життю людей, атакуючи вразливі комп'ютерні системи.

Термін «кібертероризм» - це поєднання двох понять: «кібер» («кібернетичний простір») та «тероризм». Необхідно зазначити, що зараз у науковій літературі широковживаними є терміни «віртуальний світ» та «віртуальний простір». Якщо взяти за основу поняття тероризму в поєднанні з віртуальним простором (як місцем злочину), то можна погодитись з твердженням, що «кібертероризм» – це комплексна модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту [1].

Найбільш поширеною формою здійснення кібертероризму є інформаційні атаки з боку груп та окремих осіб на електронні комунікаційні системи та мережі, комп’ютерні пристрої, бази даних та іншу мережеву і цифрову інфраструктуру. Подібні атаки дозволяють проникати глибоко в систему управління електронною комунікацією з метою перехоплення управління, викрадення/привласнення активів, або для здійснення інших деструктивних дій. В свою чергу ступінь захищеності електронних комунікацій та інформаційної інфраструктури напряму впливає на зменшення ефективності методів і форм кібертероризму.

Причини, через які кіберзлочинці атакують інформаційні системи, комп’ютерні мережі та програмне забезпечення можуть бути різноманітними: задля фінансової вигоди, розвідки або знищення даних. Країни, а також злочинні угруповання застосовують кібершпигунство для отримання конфіденційної інформації з різних галузей, таких як політика, економіка, промисловість та оборона. Це може становити загрозу національній, внутрішній і зовнішній безпеці, провокуючи конфлікти між державами.

Розвиток інформаційних технологій надає кібертерористам можливість отримувати значні прибутки практично без суттєвого ризику. Вони мають

можливість здійснювати фінансування своєї злочинної діяльності без проведення фізичних нападів або банківських пограбувань, що б демаскувало їх злочинну діяльність. Характерною рисою кібертероризму є те, що переважна більшість хакерських груп та окремих хакерів діють анонімно, використовуючи лише псевдоніми. Водночас важливо робити розмежування мж хакером-терористом та звичайним хакером-хуліганом (злодієм, шахраєм), який діє у власних корисливих інтересах або отримуючи естетичну насолоду від інформаційної атаки.

Основною тактикою кібертероризму завжди є великий суспільний резонанс, серйозні шкідливі наслідки, створення атмосфери загрози повторення, не визначаючи конкретну ціль. Наприклад, деякі лідери радикальних ісламістських організацій на Близькому Сході надають все більшого значення використанню сучасних цифрових технологій, які розглядаються ними у якості ефективної зброї в боротьбі з такими державами як Ізраїль та Саудівська Аравія, а також їз західними країнами, які надають свою підтримку цим країнам. В першу чергу, це економічний інструмент для здійснення терактів (який часто використовують країни з нерозвиненою економікою), а по-друге, кіберзлочинців відстежити доволі важко. Аналітики вважають, що більшість транснаціональних терористичних угруповань дотримуються раціонального підходу, використовуючи терор для досягнення політичних цілей і прагнучи до суспільного визнання своєї боротьби. Організаціям, що здійснюють кібернапади, потрібні висококваліфіковані виконавці, оскільки іноді кібертерористичні акти можуть мати більший ефект, ніж традиційний тероризм. Кібератаки забезпечують високий рівень анонімності й вимагають більше часу на реагування. Розробка методів протидії тероризму здебільшого стосується класичного тероризму, і кібератаки інколи можуть бути сприйняті лише як технічні збої, а не як теракти.

У сучасному світі, де глобальний кіберпростір має важливе значення для розвитку суспільних та економічних відносин, зміцнення кібербезпеки стає ключовим елементом забезпечення сталого розвитку, політичної стабільності, глобальної інформаційної безпеки тощо. Кіберзагрози стають дедалі складнішими та поширенішими, ось чому необхідність ефективних заходів для їх запобігання та

нейтралізації є критичною. Кібербезпека – це не тільки ефективні технічні рішення, але й зміни парадигми сприйняття цифрового віртуального простору людиною, тісна міжнародна співпраця та постійна освіта і власна кібергігієна. Лише за таких умов можна досягти надійного захисту в умовах постійного зростання кіберзагроз за складністю та масштабом. Надійна кібербезпека є необхідною для забезпечення стабільності, конфіденційності та безпеки у цій важливій сфері нашого життя [2].

Отже, кібертероризм є серйозною загрозою сучасного світу, що вимагає консолідації зусиль урядів, правоохоронних органів, ІТ-фахівців та суспільства загалом. Лише комплексний підхід, який поєднуватиме технологічні, законодавчі та освітні заходи, зможе ефективно протистояти цьому явищу та захистити громадян, бізнес та критичну інфраструктуру від кібератак.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради (ВВР), 2017, № 45. Документ 2163-VIII, чинний, поточна редакція — Редакція від 28.06.2024, підстава - 3783-IX. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Гриник Р.О., Пилипенко В.М. Кібертероризм як нова форма міжнародного тероризму. Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 23-25 листопада 2016 року, м. Кропивницький. – [Електронний ресурс]. – Режим доступу: https://sci.ldubgd.edu.ua/bitstream/123456789/3203/1/13.pdf

3. Атаманюк Р.Р., Копилов Е. В. Виклики та загрози в глобальному кіберпросторі: заходи з підвищення кібербезпеки у сучасному світі. Науково-дослідний інститут публічної політики і соціальних наук. Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи. Харків, 2023.

4. Рульов І.М. Кібертероризм як загроза інформаційній безпеці. Національний університет «Одеська юридична академія». – [Електронний ресурс]. – Режим доступу: https://dspace.onua.edu.ua/server/api/core/bitstreams/1a2f57d3-7b88-46ed-ab64-d4099ea8a1c5/content

МЕТЕЛЕВ Олексій Павлович
завідувач кафедри,
Національний юридичний університет імені Ярослава Мудрого

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ВИЯВЛЕННЯ ТА ПОВЕРНЕННЯ ЗЛОЧИННИХ КРИПТОАКТИВІВ У ДОХІД ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

Загальновідомо, що у тих сферах суспільного життя, де розвиваються нові відносини, там обов'язково з'являється й злочинність. Криптоактиви і блокчейн-технології останнім часом дуже швидко інтегрувались та розвинулись у багатьох сферах нашого життя. І тут мова йде не тільки про економіку: криптоактиви стали політичним, соціальним, технологічним і культурним важелем. Офіс Генерального прокурора України наголошує, що за останні 10 років кількість виявлених злочинів у кіберпросторі збільшилась майже в 8 разів, при цьому ця статистика охоплює не всі кіберзлочини, оскільки такий вид злочинної діяльності має, переважно, латентний характер і в цій злочинній діяльності в тій чи іншій мірі задіяні і криптоактиви. Звичайно, що криптоактиви стали широко використовуватись для злочинної діяльності: відмивання «брудних» коштів, забезпечення функціонування ринку наркотиків, зброї і торгівлі людьми, а останнім часом, також для обходу санкцій, спрямованих на економічну ізоляцію рф, через її неспровоковану збройну агресію проти України. Через це, постійно вживаються заходи, спрямовані на на виключення рф із числа постійних членів Групи з розробки фінансових заходів боротьби з відмиванням коштів та фінансуванням тероризму (далі – FATF) та включення рф до списку юрисдикцій високого ризику, на які поширюється заклик до дій («чорний список» FATF) [1]. Водночас, користуючись недосконалістю законодавства більшості країн світу щодо регулювання обігу криптоактивів, суб'єкти держави-агресора, як-то представники бізнесу, або державного сектору економіки, здійснюють розрахунки за підсанкційні товари та послуги за допомогою криптоактивів, створених виключно у цифровій формі, отримали можливість

ефективно впливати на відносини, що стосуються суспільно-економічного та правового напряму нашої країни.

Незважаючи на те, що в Україні вже більше 5 років фактично сформований та існує ринок криптоактивів, наразі ця сера суспільних відносин знаходиться поза межами державного регулювання. Такий стан законодавчої невизначеності дає широкі можливості для формування різного роду злочинних схем по відмиванню «брудних» коштів, торгівлі зброєю та наркотичними речовинами, фінансуванню тероризму і колабораціонізму тощо.

Саме тому, ефективність проведення санкційної політики, а також невідкладних заходів щодо запобігання та протидії загрозам національній безпеки держави, проявам тероризму та фактам поширення зброї масового ураження має пряму залежність від оперативного виявлення та припинення джерел їх фінансування (зокрема – злочинних криптоактивів), що відповідно, разом з іншими, є відповідальним напрямом реалізації положень сучасної міжнародної та національної антитерористичної стратегії, а також важливим чинником в роботі сил безпеки: правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту та інших органів, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України [2].

На наше глибоке переконання, в умовах дії військового стану, ефективність антитерористичних заходів суттєво залежить від своєчасного та системного виявлення, «замороження» джерел фінансування терористичної діяльності. Саме це є одним ключовим напрямом реалізації міжнародної та національної антитерористичної стратегії. При цьому очевидно, що в реаліях сьогодення, криптоактиви – це один із основних інструментів, яким активно користуються не тільки криміногенні угруповання всередині країни в злочинних інтересах, але й з метою зовнішнього впливу на національну безпеку.

Для ефективної боротьби з обігом злочинних криптоактивів необхідно забезпечити дієвість механізмів виявлення та повернення криптоактивів у дохід держави.

Перелічимо, на наш погляд, найбільш значущі чинники ефективного виявлення злочинних криптоактивів:

1) Технічні аспекти:

- використання технологій блокчейн-аналітики, таких як Chainalysis, Elliptic та інших;

- впровадження алгоритмів штучного інтелекту для моніторингу транзакцій [3].

2) Юридичні аспекти:

- забезпечення співпраці між правоохоронними органами та криптобіржами, обмін процесуальним досвідом реалізації кейсів, в яких фігурують криптоактиви;

- створення національних баз даних підозрілих адрес криптогаманців;

Щодо механізму повернення злочинних криптоактивів у дохід держави, то він вбачається таким:

1) Процесуальні процедури вилучення криптоактивів - які включають ідентифікацію активів на блокчейні у співпраці з криптобіржами та отримання судового рішення про арешт/замороження і конфіскацію криптоактивів.

2) Фінансово-правові механізми - які передбачають створення для відповідних державних суб'єктів спеціальних криптогаманців, з метою зберігання конфіскованих криптоактивів, а також розробка вітчизняного законодавства щодо легалізації конфіскованих криптоактивів у дохід держави, яке передбачатиме:

а) визначення статусу конфіскованих криптоактивів – тобто прийняття законів, які регулюють процедури визначення правового статусу вилучених криптоактивів, їх передачі у власність держави та можливість подальшого використання;

б) інтеграцію механізмів прозорого продажу/передачі конфіскованих криптоактивів;

в) фіскальну політику та контроль - шляхом запровадження прозорих податкових і фінансових інструментів для обліку та управління конфіскованими криптоактивами.

г) забезпечення міжнародної співпраці - узгодження з іншими країнами спільних стандартів і процедур конфіскації та обміну інформацією щодо злочинних криптоактивів.

При цьому зазначимо, що саме недостатнє законодавче регулювання у сфері обігу криптоактивів, відсутність унормованих процесуальних процедур їх блокування, вилучення та стягнення у дохід держави створює чималі перешкоди діяльності суб'єктів забезпечення національної безпеки держави.

Висновки: Ефективна боротьба зі злочинними криптоактивами в умовах воєнного стану потребує інтеграції технічних, юридичних та фінансових підходів. Необхідна тісна міжнародна співпраця для відстеження транзакцій, обміну інформацією та стандартизації процедур повернення активів. Таким чином, на наш погляд, основними шляхами виявлення та повернення злочинних криптоактивів у дохід держави є:

1) Запровадження законодавчого регулювання ринку криптоактивів в Україні.

2) Тісна співпраця з міжнародними правоохоронними органами та органами фінансового моніторингу щодо пошуку та виявлення злочинних криптоактивів.

3) Визначення та чіткий розподіл владних повноважень у сфері обігу криптоактивів серед уповноважених суб'єктів, які забезпечують національну безпеку, а також розвинення ними спроможностей, щодо: виявлення та документування злочинів, вчинених із використанням криптовалют; встановлення походження криптоактивів пов'язаних з можливою протиправною діяльністю; своєчасне та системне відстеження руху таких активів, виявлення їх місцезнаходження для подальшого блокування та конфіскації тощо.

4) Забезпечення проведення технічних та організаційних заходів щодо безперебійної роботи механізму виявлення та повернення злочинних криптоактивів.

Список використаних джерел:

1. Мінфін закликає FATF внести росію до чорного списку через подальше зростання ризиків для глобальної фінансової безпеки.

URL: https://www.mof.gov.ua/uk/news/ministry_of_finance_urges_the_fatf_to_blacklist_russia_due_to_further_growth_of_risks_for_global_financial_security-4258 (дата звернення: 15.11.2024).

2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 17.11.2024).

3. The 2023 Crypto Crime Report: 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking. URL: https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/ (дата звернення: 20.11.2024).

МИХАЙЛОВ Богдан Андрійович

студент,

Національний юридичний університет

імені Ярослава Мудрого

ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ГЛОБАЛЬНИХ ЗАГРОЗ: ВИКЛИКИ, СУЧАСНІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Забезпечення кібернетичної та інформаційної безпеки держави є критично важливим завданням в умовах сучасних глобальних загроз, пов’язаних із розвитком цифрових технологій та їх впливом на національну безпеку. Цифровізація суспільства, з одного боку, відкриває нові можливості для економічного зростання та розвитку, а з іншого — створює серйозні виклики для захисту державних і приватних інформаційних систем, критичної інфраструктури та стратегічно важливих комунікацій. Сучасні кіберзагрози, які постійно змінюються через технологічний прогрес, вимагають оперативного реагування та адаптації національних стратегій кібербезпеки. З огляду на це, забезпечення кібернетичної та інформаційної безпеки стало одним із основних елементів національної безпеки,

особливо в контексті збройних конфліктів та геополітичних криз. Враховуючи постійну еволюцію технологій, необхідно постійно оновлювати механізми захисту, а також забезпечувати інтеграцію кібербезпеки в загальну стратегію національної безпеки.

Кібербезпека є багатогранним поняттям, яке включає в себе захист інформаційних технологій і цифрових інфраструктур від несанкціонованого доступу, злому, кібератак, а також захист інформації від фальсифікації та витоку. Інформаційна безпека, у свою чергу, охоплює заходи, спрямовані на забезпечення цілісності, конфіденційності та доступності інформації, яка обробляється, зберігається або передається через електронні системи. Важливою складовою кібербезпеки є також правовий аспект, адже в умовах глобалізації кіберзагрози не знають кордонів, а міжнародне співробітництво є необхідною умовою для ефективного протистояння кіберзлочинності та кібертероризму. В Україні, зокрема, було розроблено законодавчі ініціативи, спрямовані на підвищення рівня кіберзахисту, однак ефективність їх реалізації залежить від постійного вдосконалення нормативно-правової бази, а також координації дій між державними органами та приватними структурами.

Серед основних загроз для держави в кіберпросторі виділяються кіберзлочинність, транснаціональні кіберзагрози, маніпуляції в інформаційному просторі та використання кіберзброї в рамках інформаційних війн. Кіберзлочинність є транснаціональним явищем, яке становить серйозну небезпеку для банківської сфери, енергетичних компаній, а також державних установ, зокрема через віруси, шкідливі програми та фішингові атаки. Інформаційні війни, що ведуться державами або іншими акторами на міжнародній арені, включають в себе пропаганду, дезінформацію, маніпуляції громадською думкою, а також кібератаки, які можуть мати стратегічне значення для стабільності держави. Однією з новітніх загроз є використання технологій, таких як штучний інтелект, інтернет речей і блокчейн, що, з одного боку, створюють нові можливості для забезпечення кіберзахисту, а з іншого — відкривають нові вразливості, які потребують удосконалення системи захисту даних та інфраструктури.

Розвиток кібербезпеки вимагає застосування новітніх інноваційних технологій, зокрема штучного інтелекту, машинного навчання та автоматизованих систем попередження атак. Такі технології дозволяють не тільки більш ефективно виявляти та нейтралізувати кіберзагрози, але й забезпечувати безперервний моніторинг інформаційних систем на предмет нових вразливостей. Водночас важливою є співпраця між державним та приватним секторами, оскільки багато технологій кіберзахисту розробляються та експлуатуються приватними компаніями, і їхні інновації можуть бути використані для посилення державного кіберзахисту. Крім того, ефективна система кібербезпеки потребує постійної адаптації стратегій захисту до нових технологічних реалій, що забезпечує високу ступінь гнучкості та здатність держави реагувати на непередбачувані загрози.

Перспективи розвитку кібербезпеки держави зумовлені необхідністю покращення координації між державними органами, приватним сектором та міжнародними партнерами. Удосконалення національних стратегій кібербезпеки передбачає створення нових механізмів для обміну інформацією про загрози, вдосконалення навчальних програм для підготовки кадрів, а також розвиток національних центрів реагування на інциденти. Це дозволить швидко і ефективно нейтралізувати нові загрози, мінімізуючи їхній вплив на національну безпеку та економіку. Задля підвищення готовності до кіберзагроз держави повинні регулярно оновлювати свої стратегії, проводити тренування та навчання для всіх рівнів управління, а також активно співпрацювати з міжнародними партнерами в рамках глобальних ініціатив з кібербезпеки. Тільки комплексний підхід до кіберзахисту, що поєднує інновації, ефективну правову базу та тісну співпрацю між різними секторами, може забезпечити належний рівень безпеки в умовах постійно зростаючих глобальних загроз.

Враховуючи постійну еволюцію кіберзагроз, міжнародне співробітництво стає важливим елементом у побудові ефективних стратегій кібербезпеки. Міжнародні організації, такі як ООН, НАТО, Європейський Союз, а також численні двосторонні та багатосторонні угоди, сприяють обміну інформацією про кіберзагрози, розробці спільних стандартів безпеки, а також координації заходів у разі великих

кіберінцидентів. Окремо варто відзначити необхідність розвитку інфраструктури для реагування на кіберінциденти в реальному часі, зокрема через створення міжнародних центрів моніторингу та оперативної підтримки в кіберпросторі. Така співпраця дозволяє оперативно обмінюватися інформацією про кіберзагрози, інциденти та уразливості, що дає можливість країнам швидше реагувати на атакуючі дії в кіберпросторі. Крім того, розширення застосування технологій блокчейн та криптографії на міжнародному рівні може сприяти захисту інформації від маніпуляцій та несанкціонованого доступу, забезпечуючи більшу прозорість і підзвітність операцій. Оскільки цифрові загрози є всеохоплюючими, країни повинні спільно працювати над формуванням універсальних механізмів реагування на кіберзлочинність та кібертероризм, що дозволяє швидко адаптуватися до нових викликів в кіберпросторі, підтримуючи глобальну стабільність. Важливою складовою цього процесу є створення міжнародних норм і стандартів кібербезпеки, які дозволять визначити чіткі правила взаємодії між країнами у разі кібернападів, а також забезпечать юридичні механізми для притягнення до відповідальності кіберзлочинців та тих, хто їх підтримує.

Загальні результати дослідження свідчать, що ефективне забезпечення кібернетичної та інформаційної безпеки є необхідною умовою для стабільності держави та її інтеграції в глобальну цифрову економіку. Основні рекомендації включають вдосконалення національних стратегій кібербезпеки, активізацію співпраці між державними органами, приватними компаніями та міжнародними партнерами, а також підвищення кваліфікації кадрів у сфері кіберзахисту для боротьби з новими загрозами в кіберпросторі.

Список використаних джерел:

1. Конвенція Ради Європи про кіберзлочинність (2001). – URL: https://www.coe.int/en/web/cybercrime

2. Закон України "Про основи забезпечення кібербезпеки України" (2017). – URL: https://zakon.rada.gov.ua/laws/show/2163-19

3. Андрєєв, О.І. "Кібербезпека та її роль у забезпеченні національної безпеки України". // Національна безпека України. 2020. – С. 45-58.

4. Global Cybersecurity Index (GCI) 2020. International Telecommunication Union. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

5. Захаров, І.О. "Інформаційні війни та їх вплив на національну безпеку". // Журнал міжнародних відносин, 2019. – С. 112-130.

6. Cybersecurity: The State of Play. Center for Strategic and International Studies (CSIS), 2021. – URL: https://www.csis.org/topics/cybersecurity

Закони та стратегії кібербезпеки США: аналіз та практика захисту критичної інфраструктури. – URL: https://www.cisa.gov/cybersecurity

ОХРІМОВСЬКИЙ Михайло Дмитрович

студент,

Національний юридичний університет

імені Ярослава Мудрого

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ІНСТРУМЕНТ КІБЕРЗАГРОЗ ДЛЯ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ

Сучасні інформаційні технології розширили можливості для розвитку державних структур, але водночас створили нові ризики у вигляді кіберзагроз. Одним із найефективніших інструментів, які використовуються зловмисниками, є соціальна інженерія, що дозволяє отримати несанкціонований доступ до конфіденційних даних та критичних інформаційних ресурсів. Цей тип атак націлений не на технічні уразливості, а на психологічні особливості співробітників державного сектору. Зловмисники, використовуючи обман і маніпуляції, здобувають доступ до важливої інформації, що може серйозно підірвати безпеку та діяльність державних органів. Актуальність дослідження методів соціальної інженерії для державних органів України обумовлена не лише частішими випадками

її використання, а й складними умовами, в яких перебуває держава, зокрема в умовах повномасштабного вторгнення рф. Зовнішні агресори активно застосовують комплексні методи інформаційного впливу та кібератак, серед яких соціальна інженерія відіграє значну роль у дестабілізації та підриві довіри до державних установ. За допомогою маніпулятивних методів зловмисники можуть не лише виявляти вразливі місця в державних структурах, а й реалізовувати дезінформаційні кампанії та компрометувати процеси управління і захисту національної безпеки.

Соціальна інженерія — це метод маніпуляції людьми з метою досягнення бажаних результатів, зокрема для отримання конфіденційної інформації чи здійснення небезпечних дій через зловживання психологічними та емоційними аспектами. Вона не передбачає використання технологічних уразливостей або програмних багів, а покладається на людський фактор, що робить її особливо небезпечною в умовах сучасного цифрового середовища. Особливо актуальним є питання соціальної інженерії як кіберзагрози для державних органів, де результатом таких атак може бути не тільки інформаційний витік, а й серйозний вплив на національну безпеку. У випадку атак через соціальну інженерію, навіть найсучасніші засоби захисту можуть бути неефективними, якщо співробітники не мають достатнього рівня обізнаності щодо цих загроз.

Існує кілька основних методів соціальної інженерії, що використовуються для атак на державні установи України. Фішинг є одним з найпоширеніших способів. Фішинг — це використання фальшивих електронних листів, які містять посилання на підроблені вебсайти або інші маніпуляції, що мають на меті отримати конфіденційну інформацію. Фішингові кампанії можуть бути дуже складними, включати високоякісні підробки та використовувати особисті дані цільової особи для підвищення довіри до повідомлення. У свою чергу, пре-текстинг використовує створення вигаданих ситуацій або історій, що спонукають жертву до дій, які зазвичай не здійснюються без додаткових перевірок. Наприклад, зловмисники можуть видавати себе за співробітників служби безпеки державних органів, щоб отримати доступ до системи. Вишинг (від англ. "voice phishing") полягає в телефонних дзвінках, де зловмисник прикидається представником органу влади або

іншою авторитетною особою, щоб змусити жертву надати конфіденційні дані. Це може бути використано для отримання паролів доступу до внутрішніх систем або для маніпулювання працівниками щодо виконання шкідливих дій. Смишинг (SMS phishing) використовує текстові повідомлення, що містять посилання на шкідливі вебсайти або намагаються заражати мобільні пристрої шкідливим програмним забезпеченням. В умовах масового використання мобільних пристроїв, смишинг набуває все більшої популярності серед кіберзлочинців, адже він дозволяє досягти високої результативності при мінімальних витратах на технічну реалізацію атак.

Ці методи, застосовані до державних установ, можуть призвести до витоку конфіденційної інформації, порушення нормальних функцій управлінських процесів або навіть вплинути на безпеку національних інтересів у глобальному контексті. Державні органи є одними з найбільш вразливих об'єктів для атак через соціальну інженерію. Це зумовлено тим, що багато державних установ не мають належного рівня захисту на рівні людського фактору. Найбільш уразливими є системи, що містять доступ до чутливої інформації, такі як бази даних громадян, внутрішні документообігові системи або ключові інфраструктурні компоненти. Однією з найбільших проблем є недостатня обізнаність персоналу щодо методів соціальної інженерії та слабке навчання щодо розпізнавання фішингових чи інших маніпулятивних атак. Також важливими є технічні слабкості — застарілі програмні рішення, відсутність централізованого моніторингу або слабкий контроль доступу до критичних систем. Зловмисники часто використовують ці уразливості для виконання атак. Наприклад, вони можуть надіслати співробітникам фальшиві електронні листи від імені керівництва або відомих органів влади, що змусить їх виконати шкідливі дії — від переходу за підробленим посиланням до надання доступу до внутрішніх систем через підроблені форми.

Наслідки таких атак для державної безпеки можуть бути катастрофічними. Витоки конфіденційної інформації можуть призвести до економічних або політичних криз, підриву довіри до державних інституцій, а в найгірших випадках — до національної небезпеки. Реальні приклади атак через соціальну інженерію на державні органи України підтверджують серйозність цієї загрози. Одним з таких

випадків була атака на співробітників урядових установ за допомогою фішингових листів. Зловмисники створили підроблену електронну пошту, що виглядала як офіційне повідомлення від державної установи, і вклали в лист посилання на шкідливий вебсайт. В результаті кілька працівників ввели свої дані для входу в систему, що дозволило хакерам отримати доступ до важливої інформації. Інший приклад відбувся внаслідок вишингу, коли зловмисники, видаючи себе за високопосадовців, дзвонили до представників державних структур і маніпулювали ними для отримання доступу до чутливої інформації. В результаті деякі дані були викрадені, що призвело до значних збитків та підриву довіри до системи державного управління.

Для запобігання соціальним атакам важливо впроваджувати комплексну стратегію захисту, яка включає технічні засоби, а також навички роботи з людським фактором. Сучасні методи захисту повинні включати багатофакторну автентифікацію, яка дозволяє знизити ризики, навіть якщо пароль потрапив до рук зловмисників. Важливим заходом є регулярне навчання співробітників щодо різних методів соціальної інженерії, фішингу, вишингу та інших методів маніпуляцій. Співробітники повинні знати, як розпізнавати підозрілі повідомлення та які заходи слід вжити, щоб не стати жертвами зловмисників. Іншим важливим заходом є впровадження систем моніторингу та фільтрації електронної пошти, телефонних дзвінків та текстових повідомлень, що дозволяє виявляти шкідливі повідомлення та блокувати їх до того, як вони досягнуть кінцевого користувача. Встановлення надійних антивірусних програм і систем, що перевіряють наявність шкідливого програмного забезпечення, може значно знизити ризик зараження через шкідливі вкладення або посилання.

Аналізуючи перспективи розвитку соціальної інженерії, можна відзначити, що з розвитком новітніх технологій, таких як штучний інтелект і автоматизація атак, зловмисники мають можливість створювати більш складні і переконливі маніпуляції. Штучний інтелект може бути використаний для автоматичного створення фішингових листів, дзвінків або повідомлень, які значно складніше розпізнати. Водночас постійне вдосконалення методів захисту та навчання

персоналу є важливим кроком для протидії таким загрозам. Для забезпечення високого рівня кібербезпеки державних органів необхідно розробляти комплексні стратегії, що включають як технічні, так і організаційні заходи. Вони повинні бути адаптовані до специфіки кожного окремого органу та враховувати сучасні тенденції розвитку кіберзагроз.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19.
2. Державна служба спеціального зв'язку та захисту інформації України. «Кібербезпека: актуальні виклики та загрози». URL: https://cip.gov.ua/ua/articles/cybersecurity-threats.
3. Гладка Н. М. Боротьба з кіберзлочинністю: напрями вдосконалення кримінального законодавства України [Електронний ресурс] / Н. М. Гладка // Науковий вісник Ужгородського національного університету. Серія : Право. - 2020. - Вип. 60. - С. 139-142.
4. Актуальні загрози кібербезпеки в умовах гібридної війни / В. П. Горбатюк, О. І. Селезньов // Збірник наукових праць НДІ інформатики і права. - 2021. - Вип. 5. - С. 12-16.
5. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи: монографія / А. В. Тарасюк. – Київ; Одеса: Фенікс, 2020. – 404 с.
6. Cybersecurity and Social Engineering: Methods and Threats. SANS Institute. URL: https://www.sans.org/white-papers/cybersecurity-social-engineering/.

ПОПРУЖНА Каріна Олександрівна
студентка,
Національний юридичний університет
імені Ярослава Мудрого

АНАЛІТИЧНА РОЗВІДКА В КОНТЕКСТІ ПРОТИДІЇ ТЕРОРИЗМУ ТА ЗЛОЧИННОСТІ

Аналітична розвідка відіграє ключову роль у протидії тероризму та злочинності, забезпечуючи правоохоронні та розвідувальні органи інструментами, необхідними для прогнозування, виявлення та запобігання загрозам національній безпеці. Важливість цієї теми важко переоцінити не лише для України, але й для інших країн, які стикаються із загрозою тероризму. Зростання терористичної загрози та нові виклики національній і міжнародній безпеці роблять аналітичну розвідку невід'ємною складовою стратегії національної безпеки. За допомогою аналітичної розвідки можна не лише виявити та проаналізувати потенційні загрози, але й розробити ефективні заходи протидії.

Розвідувальна діяльність – діяльність, яка 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 [1].

Що стосується саме аналітичної розвідки, то це поняття збірне як у прикладному, так і в лінгвістичному розумінні. У перекладі з грецької слово «аналіз» (analysis) означає розкладання, розчленування. Термін «аналітичний» означає «містить аналіз, детальний розбір чого-небудь», служить для аналізу [2, с. 17]. Термін «розвідка» тлумачиться як дія з метою дізнатися шляхом розпитування або спостереження про кого-, що-небудь [2, с. 1043].

Україна, враховуючи свій досвід та геополітичне положення, активно працює над удосконаленням механізмів аналітичної розвідки. Це включає посилення

міжнародної взаємодії та обміну інформацією з іншими країнами та міжнародними організаціями. Наприклад, на засіданні Ради Безпеки ООН 12 грудня 2016 року була прийнята Резолюція № 2322 [3], співавтором якої виступила Україна. Цей документ наголошує на необхідності посилення міжнародної співпраці у боротьбі з тероризмом. Зокрема, резолюція закликає держави-члени ООН до активнішого обміну розвідувальною інформацією про терористичні угруповання, включаючи біометричні дані їхніх членів. Крім того, документ підкреслює важливість співробітництва правоохоронних органів різних країн у розслідуванні та притягненні до відповідальності осіб, причетних до терористичних злочинів.

OSINT (Open Source Intelligence – розвідка з відкритим вихідним кодом) є важливим інструментом у сучасному світі аналітичної розвідки. Її методи є ключовим елементом у сфері аналітичної розвідки, яка набуває все більшого значення в сучасному світі. Вони дозволяють збирати, аналізувати та використовувати інформацію з відкритих джерел для підтримки прийняття рішень у сфері національної безпеки, оборони та розслідувань.

Джерелами такої інформації є медіа, архіви, державні документи, Інтернет та інші відкриті платформи. Завдяки технологічному прогресу, особливо розвитку Інтернету та соціальних мереж, OSINT стала дуже динамічною та мінливою галуззю, аналітичні інструменти та методи якої постійно оновлюються та вдосконалюються.

Історично OSINT сягає своїм корінням часів холодної війни, коли її використовували для аналізу інформації з відкритих джерел про військовий потенціал і політичні стратегії противника. Сьогодні OSINT включає традиційні методи, а також більш сучасні підходи, такі як супутникові знімки і аналіз великих даних. Вона відіграє важливу роль у різних сферах, від урядових і військових програм до журналістики, бізнесу, науки і освіти. Її роль особливо важлива в контексті аналітичної розвідки, яка допомагає аналітикам збирати та інтегрувати інформацію для підготовки аналітичних звітів, рекомендацій і стратегічних оцінок. OSINT також важлива для розуміння глобальних тенденцій і викликів, таких як тероризм, розповсюдження зброї, контррозвідка і кібербезпека. Вона дозволяє

аналітикам виявляти і відстежувати потенційні загрози та розробляти стратегії запобігання і реагування на них.

Важливим аспектом OSINT є етичні та правові рамки, які забезпечують конфіденційність і дотримання законодавства при зборі та аналізі інформації. OSINT буде продовжувати розвиватися, оскільки аналітики і співробітники розвідки шукатимуть нові способи використання відкритих джерел для збору цінної інформації. Зважаючи на його важливість, багато університетів та навчальних закладів пропонують курси та програми, спрямовані на підготовку фахівців у цій галузі.

Аналітична розвідка, що включає збір, аналіз та інтерпретацію даних для підтримки прийняття рішень, є ключовим елементом сучасної юридичної практики. Вона дозволяє юристам та правоохоронним органам ефективно реагувати на швидкі зміни в законодавстві та суспільстві. Однак її використання створює певні правові та етичні проблеми. Наприклад, необхідно захищати персональні дані та забезпечувати недоторканність приватного життя осіб, чия інформація збирається та аналізується. Також важливо дотримуватися принципів законності та неупередженості при використанні аналітичних методів.

Існують різні підходи до регулювання цих аспектів. Наприклад, в деяких країнах розроблені спеціальні нормативні акти, які визначають правила збору та обробки інформації. В Україні також існують законодавчі акти, які регулюють цю сферу, зокрема Закон «Про захист персональних даних» [4]. Правові норми Європейського Союзу та Ради Європи, що регулюють захист персональних даних, встановлюють вимогу щодо законної обробки цих даних. Стаття 6 (1) Загального регламенту з питань захисту персональних даних (GDPR) надає п'ять правомірних підстав для обробки даних, зокрема, якщо обробка є необхідною для виконання договору, виконання завдань в межах владних повноважень, виконання юридичного обов'язку, захисту легітимних інтересів контролера або третьої сторони, або в разі необхідності для захисту життєво важливих інтересів суб'єкта персональних даних [5].

Використання спецслужбами аналізу великих даних для виявлення потенційних терористів та їхніх планів є прикладом успішного застосування аналітичної розвідки. Інтегруючи різні джерела інформації, такі як списки пасажирів авіакомпаній, фінансові транзакції та комунікаційні дані, аналітики можуть виявити підозрілі моделі поведінки, що вказують на терористичну діяльність. Це дозволяє правоохоронним органам швидко реагувати і запобігати потенційним загрозам безпеці. Крім того, аналітична розвідка також використовується для боротьби з організованою злочинністю. Аналізуючи телефонні дзвінки, електронні листи та інші форми комунікації, можна виявити злочинні мережі та їхніх лідерів. Такий підхід не лише допомагає розслідувати кримінальні правопорушення, а й запобігає їм, розриваючи зв'язки між правопорушниками та їхніми джерелами.

Таким чином, використання аналітичної розвідки для боротьби з тероризмом і злочинністю є важливим інструментом у сучасному світі, де правопорушники і терористи постійно адаптуються до мінливих обставин і використовують новітні технології для здійснення своїх дій. Належне використання та аналіз даних може значно підвищити ефективність правоохоронних органів у їхній постійній боротьбі за підтримання безпеки та порядку.

Список використаних джерел:

1. Про розвідувальні органи України. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2331-14#Text (дата звернення: 15.10.2024).

2. Великий тлумачний словник сучасної української мови / упоряд. і голов. ред. В.Т. Бусел. К.; Ірпінь: ВТФ: Перун, 2004. 1440 с.

3. S/RES/2322(2016). *EsubscriptionUi*. URL: https://undocs.org/Home/Mobile?FinalSymbol=S/RES/2322(2016)&Language=E&DeviceType=Desktop&LangRequested=False (дата звернення: 15.10.2024).

4. Про захист персональних даних. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 15.10.2024).

5. Загальний регламент про захист даних (GDPR) - GDPR-Text.com. *GDPR-Text.com - GDPR Text, Translation and Commentary*. URL: https://gdpr-text.com/uk/ (дата звернення: 15.10.2024).

СОЛОНІНКА Михайло Петрович
студент,
Національний юридичний університет
імені Ярослава Мудрого

НЕОБХІДНІСТЬ ЗАКОНОДАВЧОГО ЗАКРІПЛЕННЯ ЦИФРОВИХ ПРАВ В УКРАЇНІ

Сучасний розвиток цифрових технологій та їх інтеграція в усі сфери суспільного життя створюють нові виклики для правової системи. Зростання обсягу цифрової взаємодії, використання персональних даних та впровадження електронного урядування обумовлюють необхідність формування комплексного законодавчого регулювання цифрових прав. В Україні, на тлі швидкої цифровізації, відсутність чіткої нормативно-правової бази щодо цифрових прав громадян породжує численні ризики, включаючи порушення приватності, дискримінацію та обмеження доступу до цифрових благ.

Актуальність роботи обумовлена потребою забезпечення балансу між розвитком цифрових технологій та дотриманням основних прав і свобод людини. Метою дослідження є аналіз необхідності законодавчого закріплення цифрових прав в Україні як ключового етапу в гармонізації національного законодавства з європейськими стандартами та забезпеченні правової визначеності в умовах цифрової трансформації.

Поняття «цифрові права» отримало різні інтерпретації у світовій науковій і правовій практиці, що відображає багатогранність і складність цього явища. Основні підходи до розуміння даного поняття наступні:

1. Одні фахівці розглядають цифрові права як адаптацію класичних прав людини до умов цифрової епохи, зокрема свободи висловлювань, права на приватність і доступ до інформації.

2. Інші вважають, що це нова категорія прав, яка включає як фундаментальні права з онлайн-складовою, так і ті, що виникли виключно у цифровому середовищі, наприклад, право бути забутим чи право на Інтернет.

3. Деякі дослідники акцентують увагу на цифрових правах як інструменті захисту прав людини в мережі, включаючи захист персональних даних і боротьбу з онлайн-дискримінацією.

4. Інша позиція полягає в розгляді цифрових прав як частини ширшої категорії інформаційних прав, але з окремими рисами, які потребують самостійного правового регулювання [5, С. 36-38].

Спільним для більшості підходів є ідея, що цифрові права – це не лише адаптація традиційних прав до нових умов, але й включення нових прав, таких як право бути забутим чи право на Інтернет. Проте відсутність єдиного визначення ускладнює їх систематизацію та правове регулювання. Ми пропонуємо визначати «цифрові права» як комплексну, самостійну групу прав людини, що пов’язана із використанням цифрових технологій, їхньою реалізацією та захистом в онлайн-середовищі.

У сучасній правовій доктрині цифрові права людини класифікують за різними підходами, зокрема залежно від сфери їх застосування, об’єктів захисту чи функціонального призначення. Узагальнивши надані погляди, можна виділити такі основні групи цифрових прав:

1. Доступ до цифрового середовища, що включає право на доступ до Інтернету, право на цифровий зв’язок та право на доступ до державних електронних послуг.

2. Приватність та захист даних, що включає право на приватність і захист персональних даних, право бути забутим та право на анонімність.

3. Свобода самовираження і участь у демократичному житті, що включає свобода вираження поглядів онлайн та право на мирні зібрання, асоціації та використання електронних інструментів демократії.

4. Безпека в цифровому середовищі, що включає право на свободу та особисту безпеку онлайн та захист від онлайн-насильства, дискримінації та інших протиправних дій.

5. Пов’язані з використанням цифрових технологій, що включає право на електронний цифровий підпис, право на створення і використання інформаційних систем та мереж та право на участь в обороті майна в цифровій сфері.

6. Нові специфічні цифрові права включають право на цифрове самовизначення, право на цифрову освіту та доступ до знань та права, пов’язані із захистом генетичної інформації [1, С. 473-475] Така класифікація охоплює базові права людини в цифровому середовищі, доповнені новими специфічними правами, що виникають унаслідок розвитку технологій. Її застосування дозволяє систематизувати підходи до захисту цифрових прав і сприяє їх ефективному закріпленню на законодавчому рівні. Необхідно зауважити, що вказані права можуть змінюватись або доповнюватись у зв’язку з інноваціями в цифровому середовищі.

Щодо закріплення цифрових прав в українському законодавстві. У контексті Європейського Союзу цифрові права закріплено в таких ключових документах, як Загальний регламент із захисту даних (відомий як GDPR), Європейська декларація про цифрові права та принципи (далі – Декларація), Європейський кодекс електронних комунікацій та інші. Декларація, ухвалена у 2023 році, стала одним із основних актів, що визначають права людини у цифровому просторі. Документ став політичною платформою для держав-членів ЄС, наголошуючи на рівності прав онлайн та офлайн, підкресленні свободи вираження поглядів, права на приватність та боротьби з дезінформацією і кіберзагрозами. Цей підхід спрямований на

створення гармонізованого цифрового середовища, де людина залишається в центрі уваги [4, С. 209-211].

Досвід інших держав також є важливим для розуміння механізмів реалізації цифрових прав. Наприклад, у Фінляндії ще в 2010 році право на доступ до Інтернету було закріплено законодавчо як базова послуга зв'язку [2, С. 104]. Франція зробила доступ до Інтернету частиною конституційної свободи вираження поглядів [3, С. 59-60]. Ці прецеденти демонструють, як цифрові права можна інтегрувати в національні правові системи для забезпечення фундаментальних свобод у сучасному світі.

В Україні цифрові права поки що не отримали належного нормативного закріплення, хоча суспільство активно інтегрується у глобальне цифрове середовище. Відсутність чітких правових гарантій створює ризики для реалізації базових прав людини в мережі Інтернет, особливо в умовах воєнного стану. Такі виклики, як кіберзагрози, маніпуляція інформацією, захист персональних даних та боротьба з дезінформацією, вимагають оперативного реагування. Крім того, закріплення цифрових прав є критично важливим для забезпечення рівного доступу громадян до цифрових ресурсів, включаючи освітні та соціальні сервіси. Європейський досвід свідчить, що відсутність цифрових прав може негативно вплинути на економічний розвиток, оскільки цифрова нерівність перешкоджає інноваціям і доступу до глобальних ринків. Ми пропонуємо наступні кроки для втілення цифрових прав в національному законодавстві:

прийняти відповідний закон про цифрові права, який чітко визначить їх перелік, механізми захисту та відповідальність за порушення. Закон має враховувати такі аспекти, як:

- право на доступ до Інтернету як базову послугу;
- захист персональних даних та конфіденційності;
- недискримінаційний доступ до цифрових ресурсів;
- право на безпеку у цифровому середовищі.

При цьому, запозичення кращих практик ЄС, зокрема впровадження інституту Уповноваженого із захисту цифрових прав громадян, подібного до європейських омбудсменів, допоможе якнайкраще втілити та захистити цифрові права на національному рівні.

Цифрові права є невід'ємною складовою сучасного суспільства, і їх закріплення в Україні є критично важливим для забезпечення основних свобод людини у цифровому середовищі. Європейський досвід, зокрема Декларація про цифрові права, демонструє, що комплексне правове регулювання сприяє соціальному та економічному розвитку. Україна має адаптувати цей досвід до своїх реалій, створивши законодавчу основу для цифрових прав, що відповідатиме сучасним викликам і потребам суспільства.

Список використаних джерел:

1. Тверезовська К.С. Поняття види та значення цифрових прав людини Юридичний науковий електронний журнал № 6, 2024. С. 472-476. URL: http://www.lsej.org.ua/6_2024/120.pdf (дата звернення 29.11.2024)
2. Ямненко Т., Міська Д. Розвиток цифрових прав в Україні. Юридичний вісник № 4(65), 2022. С. 101-106.URL: https://jrnl.nau.edu.ua/index.php/UV/article/view/17045 (дата звернення 29.11.2024)
3. Братасюк О. Б., Ментух Н. Ф. Поняття та класифікація цифрових прав в Україні. Юридичний науковий електронний журнал № 10, 2021. С. 58-61.URL:https://ccu.gov.ua/sites/default/files/bratasyuk_o.b._mentuh_n._f._ponyattya_ta_klasyfikaciya_cyfrovyh_prav_v_ukrayini.pdf (дата звернення 29.11.2024)
4. Коломоєць Т. Цифрові права людини в умовах розвитку штучного інтелекту та глобалізації. Humanities Studies № 20(97), 2024. С. 207-217. URL: http://humstudies.com.ua/article/view/312143/303213 (дата звернення 29.11.2024)
5. Бжезинський З., Братасюк О., Варламова Н., Верлос Н., Какколи Д., Карташин В., Катц, Р. До питання про юридичну природу та сутність цифрових прав людини. Правові новели № 22, 2024. С. 36-44. URL: http://legalnovels.in.ua/journal/22_2024/7.pdf (дата звернення 29.11.2024)

СТАРОСТІН Олексій Юрійович
старший викладач,
Національний юридичний університет
імені Ярослава Мудрого

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЦИФРОВОЇ ІДЕНТИЧНОСТІ ЛЮДИНИ У МЕРЕЖІ ІНТЕРНЕТ

На сьогодні помітно підвищилась роль інформаційних технологій у різноманітних сферах життя людини, як от: використання державних реєстрів для доступу до певної особистої інформації (додатки «Дія», «Резерв+», особистий кабінет платника податків тощо); соціальні мережі та месенджери для спілкування; сервіси електронної пошти; електронні кабінети пацієнтів приватних медичних закладів, з доступ до медичних записів; комерційні сервіси компаній по наданню кур'єрських послуг, таксі, придбанню та доставки продуктів харчування тощо; отримання дистанційної освіти, фінансових послуг (банки, кредитні союзи, біржі). У свою чергу доступ до електронних сервіс передбачає надання людиною персональних даних з подальшою обробкою інформації та її зберіганням за допомогою використання комп'ютерних систем, програмного забезпечення та мереж.

Водночас стрімка цифровізація самого суспільства та суспільних відносин, відносин на рівні громадянин – держава, громадянин – бізнес, призвела до обробки персональних даних, яка стала настільки частою та повсюдною, що починає піддавати загрозам право на недоторканність приватного життя.

Загалом середньостатистичний громадянин звично підписує згоду на обробку персональних даних, при виконанні процедури з відкриття рахунків у банківських установах або, наприклад, отримання дисконтних карток у мережах магазинів тощо. Така ж ситуація відбувається з погодженням на використання конфіденційних даних

та політикою конфіденційності у різних додатках на смартфоні чи на веб-сторінках різноманітних веб-ресурсів – людина звично натискає на «погоджуюсь». Дана «звичка» вже, можна казати, що стала укоріненою у суспільстві. Люди повністю покладаються на сторонніх осіб за збереження своїх даних. Якщо у відносинах з державою, як у минулому монополіста у сфері збору, збереження, обробки персональних даних громадян, це може бути виправдано, то у відносинах з приватним сектором є доволі ризиковим явищем.

Правовий захист персональних даних в Україні передбачається Конституцією України, а саме ст. 3, 28, 30, 31, 32, 34, 35, 41, 54, 55, 64.

Закон України №2297-VI від 01 червня 2010 року «Про захист персональних даних» регламентує правові відносини, які пов'язані з обробкою та захистом персональних даних. Стаття 2 даного закону містить визначення термінів, що вживаються в ньому. Так, персональні дані визначено як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Слід зауважити, що дане визначення має недолік, бо не містить чітких критеріїв, які дають можливість відокремити певні персональні дані від будь-яких іншої конфіденційних даних людини (як приклад: технічні характеристики смартфону; певна інформація про розташування особи, навіть коли служби геоданих вимкнено в налаштуваннях смартфону; інформація з файлів cookies та подібних технологій).

Захищеність персональних даних має забезпечуватись критеріями поняття «персональні дані».

На сьогодні розповсюдженими видами інформації, що можна віднести до категорії «персональні дані», є: прізвище, ім'я та по батькові; дата й місце народження; національність; місце проживання; паспортні дані; сімейний та майновий стан; біометричні дані; біологічні матеріали; політичні погляди; освіта; етнічне походження; статеве життя; релігійні переконання. Вичерпного списку не існує, бо віднесення певної інформації до персональних даних залежить від можливості ідентифікувати особу за допомогою неї.

Загалом можна виділити наступні особливості у практиці обробки персональних даних:

1. диспропорцію у обсязі запиту персональних даних та повноважень на їх обробку – компанії просять надати згоду «одразу на все», щоб у випадку реорганізації або змін у процесів, їх робота з даними людини залишалася законною;

2. відсутність гарантії захисту персональних даних – згода на обробку персональних даних не гарантує безпеку персональних даних. У мережі існує достатньо велика кількість ресурсів з викраденими або «злитими» персональними даними (номери телефонів, email адреси, банківських реквізитів, платіжних карт, акаунтів у соціальних мережах або месенджерах, інформації з державних баз даних тощо);

3. відсутність альтернативи – особа зазвичай не має можливості впливати на зміст «згоди на обробку персональних даних», наприклад, для обмеження передачі інформації про себе третім особам;

4. неможливість відстежити надані згоди – у зв'язку з активним використання електронних сервісів чи додатків, люди регулярно змушені підписувати згоди на обробку своїх персональних даних. Це призводить до того, що особа опиняється в ситуації, коли підписала велику кількість «згод на обробку персональних даних», що містять надмірний обсягом повноважень відносно їх обробки та використання, а також є складність пригадати й установити всіх суб'єктів наданої згоди.

Велику стурбованість з питання конфіденційності особи сьогодні викликає мережа Інтернет. Кожна програма, яку ми завантажуємо, кожна платформа соціальних мереж, до якої ми приєднуємось, і кожен веб-сайт, який ми відвідуємо, збирає різноманітні дані про нас. Збереження конфіденційності персональних даних в мережі Інтернет є головною проблемою для більшості користувачів. Важливість захисту персональних даних полягає в тому, що ця інформація може бути використана для нав'язування будь-якої небажаної реклами, крадіжки грошей з банківських рахунків, оформлення кредитів на великі суми та будь-які інші види шахрайства.

Під час використання мережі Інтернет люди залишають віртуальні сліди – «хлібні крихти»: цифрову інформацію про телефонні дзвінки, про місце проживання та інші дані про своє життя. Ці аспектами життя людей можуть надати більше інформації, ніж людина сама б хотіла поділитися. Сучасні цифрові технології дають змогу досліджувати мільярди взаємодій користувачів, у ході якої вони обмінюються різноманітною інформацією або, навіть, активами.

Все частіше, для обробки персональних даних у мережі Інтернет, IT індустрія використовує технології штучного інтелекту (далі - ШІ), що дають змогу на основі сформованого алгоритму вибудувати систему ефективного аналізу великого обсягу персональних даних та прийняття швидких рішень, які часто навіть не дозволяють отримати згоду суб'єкта персональних даних на подібне використання. Висока швидкість і значні обсяги оброблюваних персональних даних з використанням ШІ не дають змоги достатньо оперативно врахувати згоду суб'єкта.

Крім того, використання ШІ часто супроводжується досить великою кількістю помилок і збоїв, що призводить до порушень прав суб'єктів персональних даних.

Розповсюдженими на сьогодні стали моделі діалогового ШІ – це технологія, що дає змогу програмному забезпеченню розуміти голосові або текстові людські розмови та реагувати на них. Традиційно спілкування людини з програмним забезпеченням обмежувалося попередньо запрограмованими вхідними потоками, коли користувачі вводять заздалегідь визначені команди або вимовляють їх. Діалоговий штучний інтелект виходить далеко за рамки цього. Він може розпізнавати всі типи мовлення і введення тексту, імітувати людське спілкування, розуміти запити різними мовами і відповідати на них. Тобто у такого виду ШІ додано розвиток абстрактного мислення, вміння розпізнавати емоційні відтінки, використання гумору, вдосконалення логіки аргументації та інших аспектів комунікації.

До відомих на сьогодні AI для спілкування є Siri, Google, Alexa, Cortana. Дані системи ШІ інтегровані в операційні системи та мають певний рівень доступу до процесів, файлів і налаштувань системи. Вони є додатковим інтерфейсом, але також можуть бути використані для спілкування на вільні теми. Дані, які проходять через

подібні моделі ШІ, у більшості процесів обробляються у хмарі, а пристрій безперервно слухає оточення в очікуванні запиту. Таким чином, дані, отримані під час взаємодії з алгоритмом або в фоновому режимі, можуть бути використані не за прямим призначенням або для створення профайлів користувачів. Постійне слухання алгоритмом дозволяє визначити актуальні теми або товари для конкретної особи, що може бути застосовано в маркетингових цілях та рекламі.

Так, у вересні 2024 року, у мережі [4] з'явилася інформація щодо діяльності міжнародного рекламного гіганту Cox Media Group, а саме про використання своєї технології «Active Listening» («Активне Слухання») на основі ШІ для збору даних про розмови користувачів у режимі реального часу.

Як результат, після витоку даної інформації до мережі: Google видалив CMG зі свого веб-сайту партнерської програми; Meta, материнська компанія Facebook, також розпочала розслідування щодо CMG з питань порушень; Amazon заявив, що рекламний відділ компанії «ніколи не працював із CMG над цією програмою і не планує цього робити». З огляду на реакцію IT гігантів, є велика ймовірність, що ця інформація є правдвою, і «Active Listening» був у використанні.

У видаленому дописі в блозі Cox Media Group говориться, що технологія активного прослуховування цілком законна, оскільки зазвичай вона включена в умови використання різних програм десь дрібним шрифтом.

Також, якщо говорити про витік конфіденційних даних фізичної особи, то не слід забувати про такі ризики як успішні хакерські атаки на інформаційно-комунікаційні системи держави та приватного сектору. І, як наслідок, інформація може бути незаконно поширена.

Інформація завжди була важливим інструментом у боротьбі за владу, але в сучасну епоху вона є також зброєю. З розвитком інформаційних технологій та засобів масової комунікації зросли можливості зловживання зібраною інформацією про людей. З'явилися засоби швидкої обробки персональних даних, що створюють загрозу правам та інтересам людини.

Безпеки персональних даних є однією з найважливіших проблем в інформаційній сфері. Нові технології суттєво спростили процеси збору, обробки,

зберігання та передачі даних, але також створили загрози їх незаконного використання, що може призвести до порушень прав особистості.

Приватність – це поняття окреслює сферу будь-яких життєвих інтересів людини, в якій вона не ізольована від навколишнього світу, але, тим не менш, є автономною в межах своєї матеріальної та особистої власності.

Для збереження приватності та безпечного використання власних персональних даних, є кілька правил, яких слід дотримуватися користувачам Інтернету:

1. необхідно уважно читати угоди про обробку персональних даних на сайтах (політику конфіденційності), якщо такі угоди або правила відсутні, не варто довіряти важливу інформацію цьому сайту чи додатку;

2. якщо виявлено порушення законодавства в сфері захисту персональних даних, слід звертатися до відповідних наглядових органів.

3. необхідно надавати як можна менше особистої інформації при реєструванні у соціальних мережах;

4. важливо користуватися функцією обмеження доступ до перегляду інформації профілю в соціальних мережах або месенджерах користувачам мережі;

5. пильнуйте за змістом повідомлень та одержувачами;

6. під час використання послуг електронної комерції не варто прив'язувати банківську картку до платіжної системи сайту;

7. необхідно остерігатись фішингу – у чатах або на сторінках профілів, не потрібно переходити за сумнівними посиланнями або завантажувати незрозумілі файли. Ніколи не вводьте в сторонні форми логін / пароль / код автентифікації;

8. краще не зв’язувати свої акаунти в соціальних мережах між собою або до акаунтів онлайн-сервісів;

9. необхідно обов’язково блокувати контакти чи ботів, які вам надсилають незрозумілі пропозиції чи повідомлення;

10. не варто завантажувати особисті чи службові документи, фото автомобілів з номерним знаком транспортного засобу;

11. користування надійними сервісами VPN;

12. обов’язкове налаштування систем безпеки у додатках, у тому числі двофакторної автентифікації;

13. використання надійного антивірусного ПЗ.

Список використаних джерел:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 05.11.2024)

2. Про захист персональних даних: Закон України від 01 червня 2010 р. №2297-VI. / Верховна Рада Україна. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 05.11.2024)

3. Про інформацію: Закон України від 02 жовтня 1992 р. № 2657-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 05.11.2024)

4. Noor Al-Sibai. In Leak, Facebook Partner Brags About Listening to Your Phone’s Microphone to Serve Ads for Stuff You Mention «We know what you're thinking. Is this even legal? » / URL: https://futurism.com/the-byte/facebook-partner-phones-listening-microphone (дата звернення: 05.11.2024)

ТИМОФЄЄВ Антон Олександрович

старший викладач,

Національний юридичний університет

імені Ярослава Мудрого,

ORCID ID: 0000-0002-5297-5315

ЩОДО ПИТАННЯ ОТРИМАННЯ ЗАПИСІВ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ В РАМКАХ ДОСУДОВОГО РОЗСЛІДУВАННЯ

У великій кількості проваджень, які відносяться до підслідності СБ України виникає необхідність в отриманні відеозаписів з камер спостереження, з метою отримання відомостей стосовно осіб, які могли вчинити кримінальне правопорушення або були їх співучасниками. При цьому виникає ряд питань, які пов'язані з процедурою отримання таких доказів стороною обвинувачення.

Відповідно до ч. 2 ст. 93 Кримінального процесуального кодексу України (далі – КПК України), сторона обвинувачення здійснює збір доказів, зокрема, шляхом отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, які мають значення для кримінального провадження. Так як, відповідно до п. 1 ч. 2 ст. 99 КПК України такі відеозаписи є документами, слідчий має право направити запит особі, яка ними володіє, щодо їх отримання, з метою подальшого використання в рамках досудового розслідування. При цьому слід звернути увагу, що копія документа може вважатись оригіналом тільки в тому випадку, вона виготовлена слідчим, прокурором із залученням спеціаліста, відповідно до ч. 4 ст. 99 КПК України, а тому, власник має надіслати саме оригінал документа (матеріальний носій на який безпосередньо здійснювався відеозапис) для використання його в якості доказу.

Одночасно з цим, відповідно до ч. 1 ст. 245-1 КПК України, слідчий має право отримати дані показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису. Такі дії здійснюються на підставі постанови слідчого, прокурора, про що складається відповідний протокол. Відповідно до ч. 5 ст. 245-1 КПК України, зняття показань здійснюється шляхом копіювання особою, яка є власником або володільцем відповідних приладів та засобів, або копіювання такою особою за участю спеціаліста відповідних записів на носії, які надаються слідчим, прокурором. При цьому, таке копіювання має здійснюватися саме власником або володільцем інформації, в той час як ч. 4 ст. 99 КПК України зазначає, що копія документу може мати статус оригінала тільки у випадку виготовлення слідчим, прокурором із залученням спеціаліста, а не володільцем або власником відповідної інформації.

Окрім цього, слідчий може отримати інформацію з камер відеоспостереження, шляхом отримання тимчасового доступу до речей та документів, відповідно до Глави 15 КПК України. При цьому слід звернути увагу, що в разі отримання на виконання ухвали слідчого судді копій відеозаписів, а не їх оригіналів, таке копіювання слід в обов'язковому порядку здійснювати за участю спеціаліста.

На сьогодні є різні способи отримання слідчим інформації з камер відеоспостереження, які знаходяться у власності чи володінні інших осіб, які можна вважати взаємозамінними. У зв'язку з цим виникає ряд проблем, які пов'язані з використанням наданих відеозаписів в якості доказів в кримінальному провадженні, що потребує більш чіткого законодавчого регулювання в цій сфері.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 21.11.2024).

ТОКАР Єгор В'ячеславович
студент,
Національний юридичний університет
імені Ярослава Мудрого

АКТУАЛЬНІ КІБЕРЗАГРОЗИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: ВИДИ АТАК ТА СПОСОБИ ЗАХИСТУ

З постійним розвитком цифровізації та зростанням залежності державних структур від мережевих систем в умовах війни, кібербезпека та її забезпечення стає критично важливою складовою національної безпеки. Україна з 2014 року постійно стикається з чисельними кіберзагрозами, які мають потенційний вплив на державні інституції, економічну стабільність та суспільство в цілому. Ключова задача

російської федерації – знищення кібернетичної інфраструктури, отримання доступу до усіх ресурсів та виведення з ладу критичних ланок. Тому, сьогодні фахівці з забезпечення кібербезпеки, правоохоронні органи, хактивісти та інші ІТ-фахівці сумісно займаються питанням протидії ворогу. З початку повномасштабної агресії росії проти України суттєво змінилось становище кіберпростору, а кількість кібератак значно збільшилась. Саме тому це питання стоїть дуже гостро, і від того, наскільки держава та її громадяни протидіятимуть ворогу залежить стан забезпечення національної безпеки в сфері інформації. Важливість побудови ефективної системи кіберзахисту стає ключовим пріоритетом для забезпечення стабільності та суверенітету України в умовах інформаційного суспільства.

Поточні кіберзагрози містять різноманітні методи атак: від DDoS-атак, які ізолюють роботу веб-сайтів і державних сервісів до їх відключення через надмірну кількість запитів, до цілеспрямованих APT-атак, метою яких є здобуття чутливої інформації або доступу до критичних даних. Фішинг та використання шкідливого програмного забезпечення залишаються найбільш вживаними методами проникнення до державних мереж, оскільки використовують методи соціальної інженерії.

Варто зазначити, що російські хакерські угрупування які діють та під наглядом фсб, гру гш такі як: Fancy Bear, Strontium, Cozy Bear, Gamaredon, Killnet, часто здійснюють атаки різного рівня, зокрема DDoS-атаки для перевантаження державних сайтів, урядових порталів, банків, медіа та інших ресурсів. Такі атаки тимчасово виводять ресурси з ладу, перешкоджаючи доступу громадян та створюючи відчуття незахищеності та небезпеки. Однією з найвідоміших DDoS-атак є кібератака на урядові та банківські установи напередодні повномасштабного вторгнення, зокрема на веб-сайти Міністерства оборони України, Кабінету міністрів, державних банків Ощадбанк та ПриватБанк. Користувачі ресурсів мали проблеми з доступом до урядових сайтів, онлайн-банкінгу, не могли здійснювати фінансові операції. Іншою відомою DDoS-атакою є удар по ресурсу «Дія» у 2022 році, метою якого є – блокування доступу до ресурсу та отримання цифрових послуг, а також викачування персональних даних користувачів з системи. Атаки ускладнювали

доступ до критичних державних сервісів для українців, однак порталу "Дія" вдалося вистояти завдяки посиленій системі кіберзахисту.

Іншим видом атак є – використання шкідливого програмного забезпечення, такого як віруси, трояни, шифрувальники, які використовуються для ураження комп'ютерних систем, викрадення даних або шифрування важливих файлів. Одним з найвідоміших є вірус NotPetya, який у 2017 року масово розповсюджувався через бухгалтерське ПЗ "M.E.Doc", вразивши українські банки, енергетичні компанії, транспортні системи, медіа та інші державні установи. Також, роком раніше у 2016 році вірус Industroyer був використаний для атаки на українські енергетичні мережі, тим самим викликав тимчасове відключення електроенергії, що також спричинило суттєві збитки.

Фішинг та соціальна інженерія також входить до інструментарію ворога для здійснення кібероперації. Атаки даного типу використовуються для отримання облікових дані українських державних службовців, військовослужбовців та інших осіб, у яких ворог може бути зацікавленим. Зазвичай, здійснюється створення підроблених електронних повідомлень, або ж веб-сайтів, що виглядають як офіційні, для збору конфіденційної інформації. Ці дані є – чутливими, і можуть бути використані для маніпуляцій, шантажу, тощо.

Хакерські угрупування рф часто проводять також APT-атаки, які дозволяють ворогу доволі тривалий час залишатися непоміченими в мережі, а також розвідувальну інформацію та отримуючи доступ до конфіденційних даних, що за своєю сутністю схоже на кібершпигунство. Зокрема, хакерські групи здійснюють спроби викрасти інформацію, яка відноситься до військових операцій, політичних рішень та економічних даних за допомогою троянів, бекдорів та інших засобів, які дозволяють приховано збирати дані. Найвідомішим прикладом є атака групи Sandworm на енергосистему України, зокрема атаки на Київенерго в грудні 2015 та 2016 роках які спричинили перші блекаути. В результаті чого було відключено 30 вузлових підстанцій від яких живиться низка стратегічних об'єктів на Київщині, та вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин на Прикарпатті.

Усі ці атаки є критичними для держави, саме тому стало нагальним питанням розробки стратегії кібербезпеки, яка була вперше розроблена та впроваджена РНБО у травні 2021 року. У цій стратегії визначено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Одним з ключових нормативно-правовим актом для такої є Розпорядження Кабінету Міністрів України від 19.12.2023 № 1163 «Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України», який є стратегічно важливим і має бути виконаним в обов'язковому порядку.

Також іншими способами забезпечення кібербезпеки є - інтеграція міжвідомчих центрів реагування на кіберзагрози, при якій здійснюватиметься ефективна координація між правоохоронними органами, державними установами, банками, телекомунікаційними компаніями та іншими важливими галузями, і оперативно виявляти та реагувати на кіберзагрози.

Вкрай важливо здійснювати міжнародне співробітництво та використовувати сучасні технологій, отримувати від партнерів нові технології, знання, брати участь у міжнародних заходах для забезпечення кібербезпеки, використовувати штучний інтелект та квантову криптографію для шифрування.

Такі рішення дозволять ефективніше виявляти та реагувати на кіберзагрози, зберігати конфіденційні дані та системи у робочому стані, і таким чином – забезпечувати національну безпеку у кібернетичному просторі.

Підбиваючи підсумок, забезпечення кібербезпеки як однієї зі складових національної безпеки - є доволі складним процесом, який вимагає координованості та оперативності на державному, міжнародному та індивідуальному рівнях. Україні та її громадянам необхідно не лише захищатися від поточних загроз, а також активно розвивати інфраструктуру кібербезпеки, щоб протистояти новим викликам та загрозам у майбутньому.

Список використаних джерел:

1. Енді Ґрінберг. Піщаний хробак, або SANDWORM. Нова епоха кібервійни. Полювання на найвіртуозніших хакерів Кремля / Енді Ґрінберг. Харків: Фоліо, 2020 – 421 с.
2. Юрій Когут. Електронна книга Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології) / Практичний посібник. Юрій Когут. К.: Консалтингова компанія Сідкон, 2022 – 284 с.
3. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України".
4. Кібератака на енергетичні компанії України. Вікіпедія. Режим доступу: https://uk.wikipedia.org/wiki/ Кібератака_на_енергетичні_компанії_України.

УНГУРЯН Максим Дмитрович
студент,
Національний юридичний університет
імені Ярослава Мудрого

ПРОТИДІЯ ІНФОРМАЦІЙНИМ ВПЛИВАМ ТА ДЕЗІНФОРМАЦІЙНИМ КАМПАНІЯМ У ЦИФРОВОМУ СЕРЕДОВИЩІ

В епоху цифровізації інформаційний простір це ключова арена для ведення гібридних війн. Дезінформаційні кампанії та інформаційні впливи можуть завдати значної шкоди державній безпеці, підірвати довіру громадськості до урядових структур та навіть викликати політичну нестабільність. За даними звітів кібербезпекових агентств, кількість таких атак зростає щороку, а методи їх реалізації стають все більш складними і витонченими.

Враховуючи вище сказане вважаю актуальним визначити такі цілі даної тези:

Визначити основні типи інформаційних впливів та дезінформаційних кампаній у цифровому середовищі.

Розробити методологію виявлення та оцінки ризиків, пов'язаних з дезінформаційними атаками.

Проаналізувати сучасні методи захисту та протидії дезінформації на національному та міжнародному рівнях.

Розробити рекомендації для покращення системи інформаційної безпеки держави.

Основними загрозами та викликами для нашої держави вважаю:

Дезінформація - свідоме поширення неправдивої або маніпулятивної інформації з метою спотворення суспільної думки. Це може бути використано для підриву довіри до уряду, впливу на виборчі процеси, створення паніки в суспільстві [1].

Фейкові новини - це один із інструментів дезінформації, що відрізняється неправдивим змістом і спрямований на дезорієнтацію споживачів інформації. Фейкові новини часто містять сенсаційні заголовки, не відповідають змісту статті та поширюються через анонімні або ненадійні джерела, з метою викликати емоційну реакцію або маніпулювати суспільною думкою [2].

Інформаційні впливи через соціальні мережі включають використання таких платформ, як Facebook, Twitter, TikTok або Instagram, для поширення маніпулятивного контенту, що апелює до емоцій аудиторії. Це можуть бути пости, що викликають страх, ненависть або недовіру, часто спрямовані на підрив інформаційної безпеки або розпалювання соціальної напруги [3].

Ботоферма - це група програмних роботів (ботів), які автоматично виконують певні завдання в Інтернеті, зазвичай у великих кількостях. В контексті розповсюдження фейкової інформації, ботоферми використовуються для масового поширення маніпулятивних новин, дезінформації та пропаганди через соціальні мережі. Їх головна мета - вплив на громадську думку та маніпуляція настроями користувачів [4].

Пропоную такі методи виявлення дезінформації:

Один з найпростіших та найдієвіших методів виявлення неправдивої інформації, що передбачає аналіз достовірності фактів у статті чи пості це «фактчекінг» або просто перевірка фактів. Цей метод базується на перевірці джерел а саме: оцінкці надійності джерела інформації, перевірка попередньої репутації автора та сайту.

Також ми можемо згадати і аналіз зображень та відео, адже часто дезінформація супроводжується маніпулятивними зображеннями або відео, які змінюються або вириваються з контексту. Для виявлення такого контенту можна використовувати реверсивний пошук зображень використання інструментів, таких як Google Images або TinEye, для перевірки, чи було зображення опубліковане раніше в іншому контексті. А для виявлення діпфейків можна використати сучасні алгоритми, такі як Deepfake Detection Model, вони аналізують рухи обличчя та очей, синхронізацію звуку та відео, щоб виявити підробки.

Також в наш час доцільно використовувати штучний інтелект для виявлення та протидії дезінформації. Алгоритми штучного інтелекту здатні автоматично виявляти фейковий контент завдяки аналізу тексту, зображень та метаданих:

Аналіз тексту за допомогою NLP (обробка природної мови): визначення емоційного забарвлення, пошук стилістичних аномалій, які характерні для фейкових новин.

Методи класифікації: алгоритми, такі як Support Vector Machine, Random Forest та Long Short-Term Memory, використовуються для аналізу текстових даних та виявлення фейкових новин на основі специфічних характеристик.

Глибинне навчання: використання нейронних мереж для обробки великих обсягів даних і виявлення прихованих патернів, характерних для неправдивого контенту.

Для розпізнання ботоферми ми можемо використати аналіз активності акаунтів. Боти зазвичай мають аномально високу активність, багато лайків і репостів за короткий проміжок часу. Контент від ботів часто має шаблонний або повторюваний характер, з орфографічними помилками або неправдивою інформацією.

Розглянемо методи протидії дезінформації:

Не лише для протидії а і для виявлення дезінформації, важливо підвищувати обізнаність користувачів щодо розпізнавання фейкових новин. Це може бути як навчання людей критичному мисленню та аналізу інформації так і залучення громадськості до активної перевірки інформації та боротьби з дезінформацією. Також це може бути включення курсів з медіаграмотності у шкільну та університетську програму, а також організація тренінгів для дорослих.

Регулювання контенту та законодавчі заходи такі країни, як Німеччина та Франція, запровадили закони, що накладають штрафи на платформи соціальних мереж, які не видаляють фейковий контент протягом визначеного часу.

Також це може бути співпраця з технологічними компаніями. Такі компанії можуть впроваджувати алгоритми виявлення фейків з використанням штучного інтелекту для аналізу контенту та виявлення аномальної активності, пов’язаної з розповсюдженням фейкових новин, що допоможе в протидії вищезгаданим ботофермам. Також це можуе бути співпраця технологічних компаній з урядом та незалежними організаціями для розробки стандартів протидії дезінформації та забезпечення прозорості у процесі видалення фейкового контенту.

На мою думку дезінформація є складним і багатогранним явищем, яке становить серйозну загрозу для інформаційної безпеки держави, демократії та суспільного спокою. В умовах глобальної цифровізації та швидкого поширення контенту через соціальні мережі, фейкові новини та маніпулятивний контент можуть мати значний вплив на громадську думку, викликати паніку та спричиняти політичну дестабілізацію. Для ефективної протидії дезінформації необхідний комплексний підхід, що включає освітні, технологічні та законодавчі заходи.

Список використаних джерел:

1. ДЕЗІНФОРМАЦІЯ: ПОНЯТТЯ, ОЗНАКИ, ПЕРСПЕКТИВИ ПРОТИДІЇ, Павленко Т.А., к. ю. н., доцентка, доцентка кафедри державно-правових дисциплін, кримінального права та процесу. URL: http://www.lsej.org.ua/7_2022/80.pdf

2. ФЕЙКОВІ НОВИНИ ЯК НОВІТНІЙ ЗАСІБ МАНІПУЛЯЦІЇ ТА ДЕЗІНФОРМАЦІЇ, Доскіч Людмила Степанівна, кандидат політичних наук. URL: https://journals.uran.ua/bdi/article/view/269809

3. ДЕЗІНФОРМАЦІЯ В СОЦІАЛЬНИХ МЕРЕЖАХ: АЛГОРИТМИ ПРОТИДІЇ, Літвінчук І. С. URL: https://www.philol.vernadskyjournals.in.ua/journals/2023/1_2023/part_2/29.pdf

4. ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ ЯК ОСНОВНА ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ, Алла БАРТЕЛЬОВА URL: https://library.pp-ss.pro/index.php/ndippsn_20231212/issue/view/ndippsn_20231212/pdf

ДЛЯ НОТАТОК

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ДОКАЗУВАННЯ ПО ЗЛОЧИНАМ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Матеріали Всеукраїнського круглого столу

(м. Харків, 23 листопада 2024 року)

Видається в авторській редакції

61002, м. Харків, вул. Мироносицька, 71,
Телефон / факс: (057)700-34-55
E-mail: ipuk@ssu.gov.ua