ЗБІРНИК
«НАУКОВИЙ ВІСНИК НДІ ПРОБЛЕМ ДОСУДОВОГО РОЗСЛІДУВАННЯ» 2023-2
ISSN 2786-7900
https://doi.org/10.61417/2786-7900.2023.2.1

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ ПРОТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: НОТАТКИ НА БЕРЕГАХ ПРОЄКТУ НОВОГО КК

УДК 343.2

Рубащенко Микола,
кандидат юридичних наук,
доцент кафедри кримінального права
Національний юридичний університет
імені Ярослава Мудрого,
м. Харків, Україна

Стаття присвячена проблемам вдосконалення правового забезпечення охорони безпеки електронних комунікаційних систем, електронних мереж та комп'ютерних даних, як частини інформаційної безпеки. Здійснено аналіз положень розділу 7.7 Проєкту нового Кримінального кодексу України на предмет їх системної узгодженості між собою, з іншими положеннями Проєкту та регулюючим законодавством у сфері інформаційної безпеки, а також їх відповідності існуючим доктринальним підходам.

Ключові слова: кримінальна відповідальність, кримінальне правопорушення, інформаційна безпека, кіберзлочини, кримінальні правопорушення проти суспільства, діяння щодо комп'ютерних даних

ISSN 2786-7900

Рубащенко Н.А. Уголовные правонарушения против информационной безопасности: заметки на берегах проекта нового УК Украины

Статья посвящена проблемам совершенствования правового обеспечения безопасности электронных коммуникационных систем, электронных сетей и компьютерных данных, как части информационной безопасности. Проведен анализ положений раздела 7.7 Проекта нового Уголовного кодекса Украины на предмет их системной согласованности между собой, с другими положениями Проекта и регулирующим законодательством в сфере информационной безопасности, а также их соответствия существующим доктринальным подходам.

Ключевые слова: уголовная ответственность, уголовное правонарушение, информационная безопасность, киберпреступления, уголовные правонарушения против общества, деяния относительно компьютерных данных

CRIMINAL OFFENSES AGAINST INFORMATION SECURITY: NOTES ON THE SHORES OF THE PROJECT OF THE NEW CRIMINAL CODE OF UKRAINE

Mykola Rubashchenko,
Doctor of Law,
Associate Professor of the
Department of Criminal Law
Yaroslav Mudryi National Law University

The article is devoted to the problems of improving the legal security of electronic communication systems, electronic networks and computer data, as part of information security. An analysis of the text of section 7.7 of the Project of the new Criminal Code of Ukraine was carried out in relation to the following aspects: systematic coordination with each other, coordination with other articles of the Project and regulatory legislation in the field of information security, as well as their compliance with existing doctrinal approaches.

ISSN 2786-7900

The scope of the term «information security» used in the title of the section is much narrower than that traditionally defined in normative and doctrinal sources.

Information security, however, is harmed or threatened by many information actions provided for in other sections of the Special Part of the Project, not only by computer crimes and misdemeanors.

It seems questionable to establish criminal liability for the dissemination of false news by the person responsible for the release of the news, due to the high risk of a chilling effect on freedom of expression. The weak differentiation of responsibility for both intentional and negligent crimes on the basis of harm (consequences of the act) and the complete absence of such differentiation for misdemeanors also gives rise to criticism. The article on dealing with malicious software or hardware, which is an analogue of conventional «misuse of devices», needs improvement.

«Action regarding computer data» has a complex structure (illegal interference + other action). There is a need to ensure the punishment of illegal interference in the work of information, electronic communication, information and communication systems and electronic communication network, which was committed with the aim of destroying, blocking or distorting computer data, violating the order of their routing or processing, but if such aim is not was achieved.

Keywords: criminal responsibility, criminal offense, information security, cybercrimes, criminal offenses against society, actions related to computer data

Постановка проблеми. У 2019 році була створена Робоча група з питань розвитку кримінального права, результатом роботи якої став цілісний документ – Проєкт нового Кримінального кодексу України (далі – Проєкт) [12]. Текст Проєкту сприймається юридичною спільнотою неоднозначно, висловлюються різні, часто протилежні оцінки. Незалежно від подальшої долі цього документа наразі можна ствердно зазначити таке. По-перше, Проєкт став подією у вітчизняній науці кримінального права, яка оновила та

ISSN 2786-7900

оживила наукові дискусії, стала істотним імпульсом в його розвитку. По-друге, він однозначно є прогресивним, містить багато новел, долає низку недоліків чинного кримінального закону та пропонує оригінальні, такі що не мають аналогів, підходи до його побудови. Разом з тим, низка його положень викликають критичні судження, у тому числі й стосовно розділу 7.7 «Кримінальні правопорушення проти інформаційної безпеки».

Цим розділом передбачено 14 статей: 1) стаття з мініглосарієм – значення термінів, вжитих у цьому Розділі (7.7.1), 2) дві статті з (особливо) кваліфікуючими ознаками – ознаки, що підвищують тяжкість злочину на два ступеня (7.7.2), ознаки, що підвищують тяжкість злочину на один ступінь (7.7.3), 3) одинадцять статей, що містять окремі склади злочинів та проступків – діяння щодо комп'ютерних даних, що спричинили майнову шкоду (7.7.4), діяння щодо комп'ютерних даних, що з необережності спричинили тяжку майнову шкоду (7.7.5), діяння в сфері телекомунікаційних послуг (7.7.6), діяння щодо інформації з обмеженим доступом (7.7.7), порушення вимог безпеки комп'ютерних даних з необережності (7.7.8), несанкціоноване використання чужого цифрового образу (7.7.9), поширення неправдивої новини (7.7.10), діяння щодо комп'ютерних даних (7.7.11), діяння щодо комп'ютерних даних, що з необережності спричинили значну майнову шкоду (7.7.12), діяння зі шкідливим програмним чи технічним засобом (7.7.13), порушення вимог безпеки комп'ютерних даних, що з необережності спричинило значну майнову шкоду (7.7.14).

У цій статті аналізується контрольний текст Проєкту станом на 30 січня 2023 року.

Аналіз останніх досліджень. Проблеми правового забезпечення інформаційної безпеки були предметом численних наукових розробок. Дослідниками цієї проблематики були О.А. Баранов, О.О. Золотар, А.І. Марущак, А.Ю. Нашинець-Наумова, О.В. Олійник, В.М. Фурашев, В. Цимбалюк та багатьох інших. Кримінально-правові проблеми вдосконалення законодавства про кримінальну відповідальність

ISSN 2786-7900

відображено в працях Д.С. Азарова, П.П. Андрушка, В.С. Батиргареєвої, М.В. Карчевського, А.А. Музики, С.О. Орлова, Н.А. Розенфельда, К.В. Юртаєвої та інших.

Метою статті є аналіз положень розділу 7.7 Проєкту на предмет їх системної узгодженості між собою, з іншими положеннями Проєкту та регулюючим законодавством у сфері інформаційної безпеки, а також їх відповідності існуючим доктринальним підходам.

Виклад основного матеріалу. ***І. Концептуальні аспекти виокремлення розділу про кримінальні правопорушення проти інформаційної безпеки***. 1. Розділ 7.7 Проєкту «Кримінальні правопорушення проти інформаційної безпеки» міститься в Книзі 7 «Кримінальні правопорушення проти суспільства». Місце розділу в Книзі 7 наводить на думку, що йдеться саме про інформаційну безпеку суспільства.

Використання поняття «інформаційна безпека» в такому засадничому акті, як Кримінальний кодекс, безсумнівно потребує обґрунтування. Як зазначається, в наукових джерелах, одна з перших проблем в сфері інформаційного права, якій присвячені численні публікації, є проблема визначення змісту поняття інформаційної безпеки, і насамперед питання її об'єктів [6, с. 18]. Це поняття було предметом дослідження в багатьох публікаціях учених різних галузей права, однак можна стверджувати, що в них сформувався доволі широкий підхід до його визначення. Так, О.В. Олійник змістовну сутність інформаційної безпеки у спрощеному вигляді зводить до комплексу превентивних дій, спрямованих на забезпечення права на інформацію і свободи інформаційної діяльності, на захист інформації і права власності на інформацію, на захист від інформації та від інформаційних впливів [7, с. 135]. В. Цимбалюк визначає інформаційну безпеку як суспільні відносини щодо створення і підтримання в належному стані нормального режиму функціонування відповідної інформаційної системи; комплекс організаційних, правових та інженерно-технологічних заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних (антропогенних) загроз, реалізація яких може порушити чи

ISSN 2786-7900

припинити життєдіяльність конкретної системи [15, с. 33]. На думку В.М. Фурашева, інформаційна безпека є станом захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням [14, с. 167-168].

Інформаційна безпека визначається як складовий компонент загальної проблеми інформаційного забезпечення людини, держави і суспільства [7, с. 133]. Будучи іманентною складовою національної безпеки, за критерієм об'єктів національної безпеки України в науці справедливо виокремлюють інформаційну безпеку держави, інформаційну безпеку суспільства та інформаційну безпеку людини [3, с. 110]. Остання визначається, зокрема, як стан і процес захищеності людини від інформаційних загроз і викликів, що забезпечує можливість людини як біологічного організму і соціальної істоти функціонувати, розвиватись, задовольняти свої потреби і досягати бажаних для себе результатів в інформаційному суспільстві [4, с. 77].

Таким чином інформаційна безпека стосується всієї тріади об'єктів національної безпеки – людини, суспільства і держави, на основі якої, зокрема, побудовано й Особливу частину Проєкту (першими передбачені розділи про кримінальні правопорушення проти людини, далі – проти суспільства, останні – проти держави). Зважаючи на те, що кримінальні правопорушення, які передбачені розділом 7.7 Проєкту, за змістом посягають не лише на інтереси суспільства, але й людей та держави, то розміщення розділу про злочини і проступки проти інформаційної безпеки в Книзі про кримінальні правопорушення проти суспільства не видається вдалим.

2. Аналіз поглядів вчених на інформаційну безпеку як таку, а також інформаційну безпеку окремих об'єктів – держави, суспільства і людини, показує, що в розділі 7.7

ISSN 2786-7900

Проєкту передбачено кримінальні правопорушення, які стосуються лише окремого (одиничного) аспекту інформаційної безпеки – безпеки комп'ютерних даних та пов'язаних з ними систем і мереж. Це обумовлює потребу в обранні вужчої за змістом назви розділу. Інформаційна безпека є станом захищеності не лише самої інформації (інформації в позитивному значенні), але й станом захищеності від інформації (інформація «зі знаком мінус»). Зважаючи на другий аспект цього поняття, до правопорушень проти інформаційної безпеки належать фактично всі інформаційні діяння, які полягають в поширенні інформації з негативним змістом – публічні заклики та поширення матеріалів із ними, виправдовування та визнання правомірними агресії та окупації, неправдиві повідомлення про загрози безпеці громадян і т.п.

Так, К.В. Юртаєва відмічає, що в чинному КК України міститься значна кількість кримінальних правопорушень, склад яких безпосередньо не передбачає використання інформаційно-телекомунікаційних систем, які проте мають визнаватися кіберзлочинами, позаяк вони пов'язані зі шкідливим контентом, наприклад, порушенням рівноправності громадян за різними ознаками, заклики до вчинення протиправних дій, розповсюдження матеріалів з такими закликами тощо [16, с. 164]. В.С. Батиргарєєва також справедливо відзначає, що крім власне комп'ютерних злочинів (розділ XVI Особливої частини КК України), в чинному КК України порушення законодавства в інформаційному просторі передбачено також і кількома десятками інших статей, розміщених в інших розділах Особливої частини [2, с. 113].

Натомість розділ 7.7 Проєкту де-факто передбачає відповідальність лише за посягання на інформаційну безпеку в першому (вузькому, технічному) аспекті її розуміння. Такі діяння в міжнародних конвенціях та чинному законодавстві України називають ще кіберзлочинами. Під останніми, згідно ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України (від 05.10.2017 № 2163-VIII) [11], розуміються суспільно небезпечні винні діяння в кіберпросторі та/або з його використанням, відповідальність за які передбачена законом України про кримінальну

ISSN 2786-7900

відповідальність та/або які визнані злочинами міжнародними договорами України. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. № ETSN185 (ратифікована ВРУ 07.09.2005 р.) фактично всі вказані в розділі 7.7. Проєкту діяння (крім як за ст. 7.7.10) [5], щоправда, в більш узагальненому форматі, відносить до кіберзлочинів І групи – правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Саме такий вузький зміст інформаційної безпеки закладається і в міжнародних стандартах ISO/IEC сімейства 27000, присвяченим різноманітним питанням забезпечення інформаційної безпеки. Згідно ISO/IEC 27000:2014 (E), під інформаційною безпекою розуміється збереження конфіденційності, цілісності та можливості застосування інформації [1].

У зв'язку з цим не варто надавати «інформаційній безпеці» в матеріальному кримінальному праві такого ж обмеженого (вузького) трактування, що охоплює лише один із її аспектів, а натомість подумати про альтернативні, конкретизовані назви цього розділу, наприклад: «Кримінальні правопорушення проти кібербезпеки», «Кримінальні правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем», «Кримінальні правопорушення проти безпеки комп'ютерних даних і електронних комунікацій» тощо.

ІІ. Аналіз окремих положень розділу 7.7 Проєкту. 1. Загалом положення розділу 7.7 Проєкту очевидно відрізняються термінологічною прогресивністю порівняно з положеннями розділу XVI чинного КК України. Разом з тим, зустрічаються терміни, стосовно яких виникають питання про доцільність їх виділення або про відповідність чинному регулюючому законодавству.

У ч.1 ст. 1.4.1 Проєкту сформульовано загальне правило щодо надання термінам, вжитим в Проєкті, того чи іншого значення: «терміни, вжиті у цьому Кодексі, які мають визначення в іншому законі, міжнародному договорі чи акті Європейського Союзу, застосовуються відповідно до свого нормативного визначення, крім випадків, передбачених частиною 2 цієї статті та іншими статтями цього Кодексу». Як убачається,

ISSN 2786-7900

потреба в наданні іншогалузевим термінам, що вживаються в Проєкті, визначення в межах окремої статті кримінального закону, може бути пов'язана з тим, що цей термін не визначений в інших нормативних актах, або він має різні визначення в нормативних актах, або ж якщо для потреб кримінального права таке визначення повинно набувати іншого (особливого) змісту. Однак, очевидно, відсутня яка-небудь потреба надавати в Кодексі значення термінам, які чітко (недвозначно) визначені в регулятивних нормативно-правових актах (напр., немає потреби визначати в Кримінальному кодексі поняття «майно», «інформація», «цінний папір» і т.д.). Тож незрозуміло, навіщо в ст. 7.7.1 Проєкту надавати значення термінам «комп'ютерні дані» (пункт 1), «несанкціоноване діяння щодо інформації» (пункт 2) та «суспільно необхідна інформація» (пункт 4), якщо ці терміни визначені в регулюючих актах та конвенціях та/або ж не створюють плутанини в правозастосуванні.

Так, визначення комп'ютерних даних очевидно запозичено з Конвенції Ради Європи про кіберзлочинність, згідно п. b ст. 1 якої, комп'ютерні дані – це будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою [5]. Простішим, але фактично про те ж саме, є визначення в Законі України «Про електронні комунікації» (п. 20 ст. 2) [8].

Поняття «несанкціонованого діяння щодо інформації» також запозичено з регулюючого Закону України «Про захист інформації в інформаційно-комунікаційних системах» [9], згідно ст. 1 якого, несанкціоновані дії щодо інформації в системі – це дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства, а під порядком доступом у свою чергу згідно цього ж Закону розуміються умови отримання користувачем можливості обробляти інформацію в системі (тобто, збирати, вводити, записувати, перетворювати, зчитувати, зберігати, знищувати, реєструвати, приймати, отримувати, передавати), та правила обробки цієї

ISSN 2786-7900

інформації. Те, що санкціонованість пов'язана з дозволом власника інформації або з іншими випадками, передбаченими законом, прямо випливає зі ст. 4 цього ж Закону.

Обсяг поняття «суспільно необхідної інформації» випливає з іншого регулюючого закону, який безпосередньо стосується аналізованої сфери. У ст. 29 Закону України «Про інформацію» регулюється поширення суспільно необхідної інформації. Згідно цієї статті, інформація є суспільно необхідною, якщо вона є предметом суспільного інтересу, а під останнім вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо [10].

У цьому ж зв'язку викликає критику використання поняття «телекомунікаційна послуга» в статтях 7.7.1, 7.7.3 і 7.7.6 Проєкту. Закон України «Про телекомунікації» від 18.11.2003 р. №1280-IV втратив чинність з набуттям чинності Закону України «Про електронні комунікації» від 16.12.2020 р. №1089-IX [8]. Разом з втратою чинності згаданим законом *de-jure* із законодавства зникли нормативні визначення понять «телекомунікаційна послуга» і «телекомунікаційна мережа». Ба більше, новим законом також внесені зміни до низки інших законів, у яких терміни «телекомунікаційна мережа» і «телекомунікаційна послуга» замінено більш сучасними та ширшими термінами «електронна комунікаційна мережа» і «електронна комунікаційна послуга», зміст яких визначається новим законом.

2. Центральним видом кримінальної поведінки, передбаченої цим розділом, є *діяння щодо комп'ютерних даних*. Цьому діянню присвячено 4 з 11 статей, які передбачають ознаки основного складу кримінального правопорушення. За змістом диспозицій статей 7.7.4, 7.7.5, 7.7.11 і 7.7.12 Проєкту діяння сформульовано за одним зразком і полягає в незаконному втручанні в роботу інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи, електронної

ISSN 2786-7900

комунікаційної мережі, яке було поєднано із а) знищенням комп'ютерних даних, б) їх блокуванням, в) порушенням їх цілісності, г) порушенням порядку їх маршрутизації або г) спотворенням процесу їх обробки. Тобто йдеться про складне (складене) діяння, що має конструкцію «незаконне втручання + хоча б один з п'яти видів діяння щодо комп'ютерних даних».

З цієї конструкції випливає те, що саме лише незаконне втручання в роботу відповідної системи/мережі не є караним. Ба більше, з огляду на те, що всі умисні злочини проти інформаційної безпеки вважаються лише злочинами 1 ступеня тяжкості, і з урахуванням того, що замах на злочин 1-2 ступеня тяжкості згідно положень Проєкту не вважається кримінальним правопорушенням (ст. 2.6.1), не буде караним і незаконне втручання, вчинене з метою знищення, блокування даних, порушення їх цілісності і т.д., якщо цілі не були досягнуті з незалежних від особи причин. Навряд чи таке положення сприятиме посиленню безпеки комп'ютерних даних. Тож, як убачається, варто замислитися над підвищенням ступеня тяжкості цих злочинів або ж над зміною положень про некараність замаху на окремі види злочину.

3. Закладений в Проєкті підхід, за яким у кожній статті може бути лише один (основний) склад кримінального правопорушення, а диференціюючі (кваліфікуючі, особливо кваліфікуючі та привілеюючі) ознаки винесено в окремі статті на початку кожного розділу, призводить до штучного дублювання одного і того ж діяння в межах декількох статей одного й того ж розділу. За того підходу, що використовується в чинному КК (диференціація відповідальності, як правило, в межах однієї статті), замість чотирьох статей можна було б сконструювати одну з декількома частинами: ч. 1 – діяння щодо комп'ютерних даних (формальний склад, проступок, ст. 7.7.11), ч. 2 – те саме, що з необережності спричинило значну майнову шкоду (проступок, ст. 7.7.12), ч. 3 – те саме діяння, що умисно спричинило істотну майнову шкоду (злочин 1 ступеня, ст. 7.7.4), ч. 4 – те саме діяння, що з необережності спричинило тяжку майнову шкоду (злочин 3 ступеня, ст. 7.7.5).

ISSN 2786-7900

4. Як убачається, системною проблемою в Проєкті є слабка диференціація відповідальності як за умисні, так і за необережні злочини за ознакою заподіяння шкоди (наслідків діяння) та повна відсутність такої диференціації за проступки. Проявляється вона і стосовно кримінальних правопорушень проти інформаційної безпеки. Складається враження, що на кримінально-правову увагу заслуговує лише шкода майнова, при чому виключно прямі збитки, виходячи з визначення цієї шкоди в загальному глосарії (п. 63 ст. 1.4.1); упущена вигода і моральна шкода врахуванню в цьому випадку не підлягатимуть. Тож поза увагою кримінального права залишаються численні випадки порушення конституційних прав і свобод людини, а також порушення законних інтересів держави, територіальної громади, юридичних та фізичних осіб, які не піддаються грошовій оцінці або така оцінка не може бути адекватною. Завдяки цьому відбувається суттєве послаблення ролі кримінального права та й можливостей права в охороні соціальних цінностей загалом.

Уникнути послабленню правоохоронної функції кримінального права дозволить використання класичних понять на кшталт «істотна шкода», «значна шкода», «тяжка шкода» і т.п., однак з конкретизацією їх змісту в такий спосіб, щоб вони охоплювали не лише майнову шкоду. Тут варто погодитися з В.І. Тютюгіним, який вважає, що роз'яснення змісту та окреслення обсягу таких понять, як «істотна шкода» і «тяжкі наслідки» має здійснюватися не до всіх норм КК в цілому, а в кожному окремому розділі Особливої частини КК, де зосереджені норми про відповідальність за відповідні злочини (напр., шляхом роз'яснення того чи іншого поняття (терміну) в одній із перших статей цього розділу) [13, с. 162].

5. За змістом статей 7.7.4 і 7.7.5 ідеться про «втручання» в роботу відповідних систем чи мережі як таке, тобто без конкретизації того, чи відбувається це законно чи незаконно, санкціоновано чи несанкціоновано. При цьому в аналогічних статтях цього ж розділу, які передбачають відповідальність за кореспондуючі проступки, використовується вже зв'язка «незаконне втручання» (див. статті 7.7.1 і 7.7.12). Ба

ISSN 2786-7900

більше, в статтях інших розділів Особливої частини, де діяння полягає у втручанні, також зустрічаємо різні варіанти – просто «втручання» (напр., статті 8.1.5 чи 8.2.3), «незаконне втручання» (напр., ст. 4.10.5) чи «несанкціоноване втручання» (напр., ст. 4.10.7). Така термінологічна неоднозначність є характерною й для чинного КК України.

Цю проблему можна вирішити різними шляхами. Найкращими видаються два з них: а) визначити термін втручання в загальному глосарії, вказавши на незаконність чи несанкціонованість такого діяння, або б) в кожному випадку використання цього слова на позначення діяння в Особливій частині зазначити про його незаконність / несанкціонованість.

6. Згідно ст. 7.7.10 Проєкту, особа, яка, будучи відповідальною за випуск новини, допустила до ефіру, тиражу або допису редакції в соціальній мережі завідомо неправдиву суспільно необхідну інформацію, – вчинила злочин 1 ступеня. Фактично, це єдина стаття з розділу 7.7, яка посягає на інформаційну безпеку в широкому її значенні, зокрема в аспекті убезпечення суспільства від дезінформації. Не викликає сумнівів, що медійники нерідко використовують свої можливості впливу на широке коло осіб в корисливих або інших особистих інтересах чи інтересах третіх осіб, зокрема, й на замовлення. Як наслідок, замість неупередженого висвітлення фактів, медійники стають знаряддям в антиконкурентній боротьбі політиків, суб'єктів господарювання тощо. Тому бажання криміналізувати випуск завідомо неправдивої новини, що визнається суспільно необхідною інформацією, можна зрозуміти.

Проте з першого її прочитання стає зрозуміло, що ця стаття насамперед стане знаряддям впливу на медіа та неодмінно призведе до охолоджуючого ефекту на свободу вираження поглядів («chilling effect on freedom of expression»), адже редактор (чи інша відповідальна за випуск особа) кожного разу перебуватиме умовно кажучи «під загрозою покарання» і для того, щоб не мати проблем з правоохоронними органами, буде намагатися оминути гостру проблему, уникати висвітлювати суспільно необхідну

ISSN 2786-7900

інформацію, яка не є достатньо перевіреною чи яка отримана з джерел, які не можна розкривати і т.д. Інакше кажучи, ця стаття не безпідставно може бути розцінена як запровадження цензури в Україні.

7. Згідно ст. 7.7.13 Проєкту, особа, яка шкідливий програмний чи технічний засіб, призначений для несанкціонованого втручання в роботу інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи, електронної комунікаційної мережі, з метою його протиправного використання, розповсюдження або збуту створила, переміщувала або збула, – вчинила проступок. Ця стаття, як можна припустити, є спробою імплементації ст. 6 Конвенції Ради Європи про кіберзлочинність («Зловживання пристроями»), згідно якої: «Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це:

a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: i) пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2 – 5 вище; ii) комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2 – 5; та

b. володіння предметом, перерахованим у підпунктах a. i) або ii) вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2 – 5…» [5].

Імплементація цієї статті Конвенції безумовно вітається, водночас, потребують вдосконалення положення Проєкту, якими вона віддзеркалюється. По-перше, стосовно передбачених у цій статті предметів, то в пунктах 6 та 7 ст. 7.7.1 Проєкту (глосарій до розділу) надано визначення термінів «шкідливий програмний засіб» та «шкідливий

ISSN 2786-7900

технічний засіб» відповідно як комп'ютерної програми або пристрою, розроблених для спричинення шкоди комп'ютерним даним, інформаційним системам та / або телекомунікаційним мережам. Іншими словами в ст. 7.7.13 відображено лише підпункт a. i), при цьому замість одного універсального визначення, надається два окремих (зайве дублювання).

По-друге, Конвенція вказує на те, що ці програми/пристрої мають мету, в першу чергу, вчинення злочинів, передбачених попередніми статтями Конвенції, у яких ідеться про втручання в систему та дані, нелегальне перехоплення та незаконний доступ. Тобто, при визначенні предмету цього правопорушення має йтися не про мету заподіяння шкоди, а про мету вчинення відповідних кримінальних правопорушень.

У цьому ж зв'язку виникає питання, чи є на стільки принциповим те, що програма чи пристрій саме створені зі злочинною метою? А якщо вони створені без такої мети (а навіть навпаки – для захисту від подібних програм чи пристроїв), але використані для злочинної мети? Натомість у Конвенції йдеться про те, що відповідний засіб може бути не лише створений, але й адаптований з метою вчинення відповідних протиправних діянь.

По-третє, неврахованим залишається підпункт a. ii), який предметом «зловживання пристроями» також визнає комп'ютерні паролі, коди доступу або подібні дані, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи.

Зважаючи на це, в глосарії до розділу 7.7 можна надати таке значення термінів: 1) «шкідливий програмний або технічний засіб – це комп'ютерна програма або пристрій, створені або адаптовані для вчинення кримінального правопорушення, передбаченого цим Розділом», 2) «дані доступу – комп'ютерні паролі, коди доступу або подібні дані, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з метою вчинення кримінального правопорушення, передбаченого цим Розділом».

По-четверте, в Конвенції рекомендується криміналізувати не лише створення, переміщення і збут, але й придбання та володіння відповідними предметами. З цього

ISSN 2786-7900

приводу власні критичні судження вже висловлювала К.В. Юртаєва [16, с. 165]. Тому потрібно доповнити статтю також придбанням з метою протиправного використання, розповсюдження або збуту предмета та володінням з метою його використання для вчинення кримінальних правопорушень, передбачених цим Розділом.

Висновки. На підставі вище викладеного, можна стверджувати, що попри прогресивність та новаторські підходи, низка положень розділу 7.7 Проєкту мають дискусійний характер та потребують удосконалення. Зважаючи на зміст діянь, передбачених цим розділом, обсяг поняття «інформаційна безпека», використаного в назві розділу, виявляється набагато вужчим за той, який традиційно визначається в нормативних та доктринальних джерелах. Безпека комп'ютерних даних, інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи та електронної комунікаційної мережі є лише частиною інформаційної безпеки. Останній однак заподіюється шкода чи створюється загроза її заподіяння й багатьма інформаційними діяннями, передбаченими іншими розділами Особливої частини Проєкту, а не лише комп'ютерними злочинами та проступками.

Потребують удосконалення окремі положення розділу 7.7: 1) визначення в глосарії понять «комп'ютерні дані», «несанкціоноване діяння щодо інформації» та «суспільно необхідна інформація» видаються зайвими, оскільки вони дублюють нормативні (у т.ч. конвенційні) положення; 2) поняття «телекомунікаційна мережа» в регулюючому законодавстві замінено на «електронну комунікаційну мережу»; 3) зважаючи на складену конструкцію «діяння щодо комп'ютерних даних» потребує забезпечення караності незаконне втручання в роботу інформаційної, електронної комунікаційної, інформаційно-комунікаційної систем та електронної комунікаційної мережі з метою знищення, блокування чи спотворення комп'ютерних даних, порушення порядку їх маршрутизації чи процесу обробки, якщо така мета не була досягнута з незалежних від волі особи причин; 4) викликає критику встановлення кримінальної відповідальності за поширення неправдивої новини, особою відповідальною за випуск новин, у зв'язку з

ISSN 2786-7900

високим ризиком охолоджуючого ефекту на свободу вираження поглядів; 5) породжує критику й слабка диференціація відповідальності як за умисні, так і за необережні злочини за ознакою заподіяння шкоди та повна відсутність такої диференціації за проступки; 6) потребує вдосконалення стаття про діяння зі шкідливим програмним чи технічним засобом, що є аналогом конвенційного «зловживання пристроями».

Література:

1. International standard ISO/IEC 27000:2014: Information technology. Security techniques. Information security management systems. Overview and vocabulary. URL: https://www.iso.org/standard/63411./

2. Батиргареєва В.С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. Інформація і право. 2020. № 1 (32). С. 110-119.

3. Золотар О.О. Класифікація інформаційної безпеки. Інформація і право. 2011. №2 (2). С. 109-113.

4. Золотар О.О. Поняття та зміст категорії «інформаційна безпека людини». Інформація і право. 2021. № 1 (36). С. 73-78.

5. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. № ETSN185.
URL: https://zakon.rada.gov.ua/laws/show/994_575./

6. Марущак А.І. Дослідження проблем інформаційної безпеки у юридичній науці. Правова інформатика. 2010. № 3 (27). С. 17-21.

7. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні. Право і суспільство. 2012. № 3. С. 132-137.

8. Про електронні комунікації: Закон України від 16.12.2020 р. №1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20./

9. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР.
URL: https://zakon.rada.gov.ua/laws/show/80/94-вр./

10. Про інформацію: Закон України від від 02.10.1992 р. № 2657-XII.
URL: https://zakon.rada.gov.ua/laws/show/2657-12./

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII.

ISSN 2786-7900

URL: https://zakon.rada.gov.ua/laws/show/2163-19./

12. Проєкт Кримінального кодексу України (станом на 30 січня 2023 року). URL: https://newcriminalcode.org.ua/criminal-code.

13. Тютюгін В.І. Деякі шляхи вдосконалення положень Кримінального кодексу України. Концептуальні засади нової редакції Кримінального кодексу України : матеріали міжнар. наук. конф., м. Харків, 17-19 жовт. 2019 р. Харків: Право, 2019. С. 161-165.

14. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2 (5). С. 162-175.

15. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2004. Вип. 8. С. 30-33.

16. Юртаєва К.В. Відповідальність за злочини та проступки проти інформаційної безпеки в проєкті КК України крізь призму принципу верховенства права. Проєкт нового Кримінального кодексу України у вимірі верховенства права: матеріали сателіт. заходу V Харк. міжнар. юрид. форуму (м. Харків, 21 верес. 2021 р.). Харків: Право, 2022.С. 164-166.