НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ВИВЧЕННЯ ПРОБЛЕМ
ЗЛОЧИННОСТІ ІМЕНІ АКАДЕМІКА В. В. СТАШИСА

МІЖНАРОДНІ СТАНДАРТИ ТА НАЦІОНАЛЬНА КРИМІНАЛЬНО-ПРАВОВА ПОЛІТИКА У СФЕРІ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Монографія

НАЦІОНАЛЬНА АКАДЕМІЯ
ПРАВОВИХ НАУК УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ВИВЧЕННЯ ПРОБЛЕМ ЗЛОЧИННОСТІ ІМЕНІ АКАДЕМІКА В. В. СТАШИСА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

До 30-річчя Національної академії правових наук України

МІЖНАРОДНІ СТАНДАРТИ ТА НАЦІОНАЛЬНА КРИМІНАЛЬНО-ПРАВОВА ПОЛІТИКА У СФЕРІ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Монографія

За загальною редакцією
В. І. Борисова, М. В. Карчевського, М. В. Шепітька

Електронне наукове видання

Харків
«Право»
2023

УДК 004.056:006.42
М58

Р е ц е н з е н т и:

Музика Анатолій Ананійович – доктор юридичних наук, професор, провідний науковий співробітник науково-дослідної лабораторії кримінологічних досліджень та проблем запобігання злочинності Державного науково-дослідного інституту МВС України, член-кореспондент НАПрН України, заслужений діяч науки і техніки України;

Радутний Олександр Едуардович – кандидат юридичних наук, доцент, доцент кафедри кримінального права Національного юридичного університету імені Ярослава Мудрого

Рекомендовано до друку вченою радою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України (постанова № 6/3 від 13 грудня 2023 р.)

Міжнародні стандарти та національна кримінально-правова полі-
М58 тика у сфері охорони інформаційної безпеки : монографія : електрон. наук. вид. / за заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. – Харків : Право, 2023. – 152 с.

ISBN 978-966-998-681-8

Монографія є результатом комплексного розгляду актуальних проблем міжнародно-правової регламентації інформаційної безпеки та формування з цього приводу національної кримінально-правової політики. Запропоновано науково-теоретичне визначення інформаційної безпеки, окреслено види суспільних відносин, що її забезпечують. Висвітлено питання реалізації міжнародних стандартів протидії кримінальним правопорушенням у сфері використання інформаційних технологій та формування інформаційного простору. Досліджено загальні засади та окремі напрями державної політики у сфері кримінально-правового забезпечення інформаційної безпеки (у тому числі в умовах воєнного стану).

Видання розраховане на науковців, викладачів права, народних депутатів України, працівників правоохоронних і судових органів, аспірантів (ад'юнктів), студентів, слухачів вищих навчальних закладів, а також усіх інших осіб, хто цікавиться цією проблематикою.

УДК 004.056:006.42

Видання в електронному вигляді розміщується у відкритому доступі на сайті НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України в розділі «Електронні джерела» (https://ivpz.kh.ua/uk/електронна-бібліотека/) вкладки «Інфопідтримка». Для опису видання чи посилання на нього слід використовувати пряме URL-посилання.

ISBN 978-966-998-681-8

ЗМІСТ

РОЗДІЛ 1
МІЖНАРОДНІ СТАНДАРТИ, РЕКОМЕНДАЦІЇ ЄС, ПРОГРЕСИВНИЙ ЗАРУБІЖНИЙ ДОСВІД ЩОДО КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

РОЗДІЛ 2
ПРІОРИТЕТНІ НАПРЯМИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КРИМІНАЛЬНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розділ 1

МІЖНАРОДНІ СТАНДАРТИ, РЕКОМЕНДАЦІЇ ЄС, ПРОГРЕСИВНИЙ ЗАРУБІЖНИЙ ДОСВІД ЩОДО КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ

Зарубіжний та міжнародний досвід – важливе джерело знань для забезпечення ефективного національного правового регулювання. У цьому питанні кримінально-правова охорона інформаційної безпеки не є виключенням. Транскордонність «кіберзлочинності», глобальні мережі, система децентралізованих фінансів – це лише деякі особливості досліджуваного виду суспільно небезпечних посягань, що актуалізують міжнародну співпрацю та взаємодію.

У цьому розділ представлені такі напрацювання: 1) проблеми кримінально-правової охорони інформаційної безпеки, що потребують дослідження міжнародного досвіду; 2) міжнародні стандарти та досвід протидії кримінальним правопорушенням в сфері використання інформаційних технологій; 3) міжнародна регламентація питань формування інформаційного простору; 4) CAN SPAM Act як приклад прагматичного підходу кримінально-правової охорони суспільних відносин інформаційної безпеки.

Для того, щоб структурувати викладений нижче матеріал, спочатку висловимося стосовно нашого розуміння поняття «інформаційна безпека», класифікуємо види суспільних відносин, які складають цей об'єкт посягання, визначимо найбільш актуальні проблеми кримінально-правової охорони відносин інформаційної безпеки в Україні. Під кутом визначених проблем проаналізуємо відповідний зарубіжний та міжнародний досвід.

1.1. Проблеми кримінально-правової охорони інформаційної безпеки, що потребують дослідження міжнародного досвіду

1.1.1. Інформаційна безпека як об'єкт кримінально-правової охорони

Необхідність кримінально-правового стимулювання позитивних та мінімізації негативних наслідків інформатизації обумовила появу відносно самостійної групи суспільних відносин, що ми будемо називати інформаційна безпека та визначимо як систему суспільних відносин стосовно реалізації інформаційної потреби особи, суспільства, держави. Ця система складається з трьох елементів: відносини в сфері використання ІТ, відносини в сфері забезпечення доступу до інформації, відносини в сфері формування інформаційного поля.

Включення поняття «інформаційна безпека» в науковий та нормативно-правовий обіг зумовлене перш за все ст. 17 Конституції України, у якій зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Закон України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р. (нині втратив чинність) містив положення про те, що інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. До об'єктів інформаційної безпеки цей закон відносив: інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни. Отже, про інформаційну безпеку в цьому нормативно-правовому акті йшлося як про комплекс заходів, спрямованих на забезпечення захисту інформації від неправомірного витоку, перекручення, знищення тощо. Чинний Закон України «Про національну програму інформатизації»,

прийнятий від 01.12.2022 р., також розглядає інформаційну безпеку в означеному контексті. До обов'язків замовників Національної програми віднесено забезпечення інформаційної безпеки держави та кіберзахист державних інформаційних ресурсів, захист інформації, вимогу щодо захисту якої встановлено законом (ст. 7).

Водночас рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки», введене у дію Указом Президента України № 685/2021, визначає інформаційну безпеку значно ширше: «інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом».

Аналогічний зміни у розумінні інформаційної безпеки відбулися й на доктринальному рівні кримінального права. Тривалий час у кримінально-правовому науковому дискурсі поняття «інформаційна безпека» переважно використовувалося у вузькому значенні: як захищеність від витоку відомостей, що містять державну таємницю. Насамперед це пов'язано з тим, що у КК воно використовується тільки в диспозиції ч. 1 ст. 111, яка передбачає відповідальність за державну зраду. Так, М. І. Хавронюк обґрунтовано зазначає, що безпосереднім об'єктом державної зради є національна безпека переважно у сфері державної безпеки, інформаційній, економічній, науково-технологічній і військовій сферах, при цьому робить уточнююче зауваження про те, що в контексті ст. 111 інформаційна безпека перш за все означає захищеність України від витоку інформації, що складає дер-

жавну таємницю[1]. Е. М. Кісілюк та В. І. Павліковський у ході аналізу складу злочину державної зради зазначають, що під загрозами національній (у тому числі державній) безпеці України в інформаційній сфері варто розуміти витік інформації, яка становить державну таємницю[2]. Подібні позиції висловлювалися й іншими дослідниками[3].

Очевидно, що таке становище не відповідає соціальним тенденціям інформатизації та зумовленим ними потребам у правовому регулюванні й охороні суспільних відносин. В умовах, коли можливі загрози у сфері інформаційної безпеки далеко не вичерпуються витоком відомостей, що складають державну таємницю, кримінальне право, як нормативна база охорони суспільних відносин від злочинних посягань, не повинне розглядати інформаційну безпеку настільки вузько.

Саме тому в наукових дослідженнях у сфері теорії права[4], основ національної безпеки[5], адміністративного права[6], кримінології та кри-

---

[1] Науково-практичний коментар до Кримінального кодексу України / За ред. М. І. Мельника, М. І. Хавронюка. 8-е вид., перероб. і доп. Х.: Фактор. 2011. С. 257–258.

[2] Кримінальне право України. (Особлива частина) : підручник / Кол. авторів А. В. Байлов, О. А. Васильєв, О. О. Житний та ін..; за заг. ред. О. М. Литвинова; наук. ред. серії О. М. Бандурка. Х. : Вид-во ХНУВС. 2011. С. 31

[3] Уголовный кодекс Украины: Научно-практический комментарий / Отв. ред. С. С. Яценко. 3-е изд., исправл. и доп. К. : А. С. К., 2004. С 256; Уголовный кодекс Украины: Научно-практический комментарий / Отв. ред. Е. Л. Стрельцов. Издание четвертое, переработанное и дополненное. Х.: Одиссей. 2007. С. 244; Кримінальний кодекс України: Науково-практичний коментар / Ю. В. Баулін, В. І. Борисов, С. Б. Гавриш та ін. За заг. ред. В. В. Сташиса, В. Я. Тація. Вид. четверте, доповн. Х. : ТОВ «Одіссей». 2008. С. 327.

[4] Тихомиров О. О. Забезпечення інформаційної безпеки як функція держави : автореф. дис. … кандидата юрид. наук : 12.00.01. К. 2011. 19 с.

[5] Горбулін В. П., Биченок М. М. Проблеми захисту інформаційного простору України : монографія / Інтситут проблем національної безпеки. К. : Інтертехнологія. 2009. 136 с.; Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) : автореф. дис. … кандидата політ. наук: 21.01.01. К. 2005. 20 с.

[6] Кормич Б. А. Інформаційна безпека: організаційно правові основи : навч. посібник. К. : Кондор, 2004. 384 с.; Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. для студ. ВНЗ. К. : КНТ, 2007. 531 с.; Ліпкан В. А. Адміністративно-правові основи забезпечення національної безпеки України : автореф. дис… доктора юрид. наук. К. 2008. 34 с.

мінального права[1], політології[2], міжнародних відносин[3] інформаційна безпека розглядається значно шире, що є закономірним відображенням значення інформаційних процесів та небезпеки відповідних посягань.

Зрозуміло, що в кожній сфері визначення інформаційної безпеки має свою специфіку. Є вона і в кримінально-правовому вимірі проблеми.

По-перше, в означеному контексті інформаційну безпеку доцільно розглядати не як певний стан або захищеність, а як систему суспільних відносин. Будь-який інший підхід входив би в очевидну суперечність з аксіоматичними положеннями юридичної науки.

По-друге, інформаційна безпека має специфічне подвійне значення, нормативно-правовий вплив на відносини інформаційної безпеки здійснюється як у межах інформаційного права, так і за допомогою різноманітних інших конструктивних галузей права: конституційного, цивільного, банківського, комерційного тощо. Відповідно, і кримінально-правова охорона забезпечується за допомогою норм, що передбачають посягання на різноманітні родові об'єкти.

По-третє, визначення інформаційної безпеки як об'єкта кримінально-правової охорони передбачає встановлення тих соціальних потреб, що зумовлюють необхідність кримінально-правової охорони. Поява та функціонування суспільних відносин інформаційної безпеки пов'язані з інформаційною соціальною потребою.

Таким чином, інформаційна безпека розуміється нами як система суспільних відносин, що забезпечує можливість реалізації інформаційної потреби громадян, суспільства, держави. Реалізація інформаційної потреби здійснюється шляхом отримання доступу до необхідної інформації, базується на використанні інформаційних технологій та забез-

---

[1] Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.; Батиргареєва В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право*. №1 (32). 2020. С. 110–119. DOI: https://doi.org/10.37750/2616–6798.2020.1(32).200388;

[2] Сащук Г. М. Безпекові імперативи телевізійного простору України : автореф. дис. … кандидата політ.наук: 23.00.03. К., 2005. 16 с.

[3] Скляренко О. А. Сучасні проблеми інформаційної безпеки України в умовах внутрішніх трансформацій. *Актуальні проблеми міжнародних відносин*. 2006. Випуск 64 (Частина І). С. 125–131.

печується формуванням інформаційного ресурсу. Означеного достатньо для того, щоб сформулювати таке визначення: інформаційна безпека – система суспільних відносин щодо забезпечення реалізації інформаційних потреб громадян, суспільства, держави, яка включає: 1) відносини щодо забезпечення доступу до інформаційних ресурсів; 2) відносини щодо формування інформаційного ресурсу; 3) відносини щодо забезпечення функціонування інформаційних технологій як засобів доступу до інформаційного ресурсу та його формування.

Суб'єкт перебуває в стані інформаційної безпеки тоді, коли ефективність його діяльності забезпечена повною, достовірною та достатньою для прийняття рішень інформацією. Такий стан досягається соціальною активністю в трьох взаємопов'язаних групах суспільних відносин, що представляють собою структурні елементи інформаційної безпеки: суспільні відносини у сфері використання інформаційних технологій, у сфері забезпечення доступу до інформаційного ресурсу й у сфері формування інформаційного ресурсу. У межах першої групи забезпечується функціонування ефективних засобів інформаційної діяльності, у межах другої – забезпечується можливість суб'єктів отримувати доступ до необхідних інформаційних ресурсів, у межах третьої – формується інформаційний ресурс, що відповідає потребам суб'єктів[1]. *Серед означених суспільних відносин ті, що охороняються законом про кримінальну відповідальність, і складають зміст інформаційної безпеки як об'єкта кримінально-правової охорони.*

1.1.2. Основні проблеми кримінально-правової охорони відносин інформаційної безпеки в сфері використання інформаційних технологій

Ключові проблеми протидії кримінальним правопорушенням у сфері використання інформаційних технологій можуть бути охарак-

[1] Карчевський М. В. До питання визначення інформаційної безпеки як об'єкта кримінально-правової охорони. *Боротьба з організованою злочинністю і корупцією (теорія і практика)* : науково-практичний журнал. 2012. №27. С. 267–272.

теризовані таким чином. По-перше, примітивізація кримінально-правової протидії − ситуація, коли значна частина судових рішень, пов'язаних із засудженням осіб за певні кримінальні правопорушення, стосується найменш небезпечних форм таких правопорушень за умови фактичної відносної поширеності більш небезпечних форм цих правопорушень. По-друге, неготовність до прогнозованого широкого використання нових видів інформаційних технологій для вчинення кримінальних правопорушень. Йдеться передусім про використання віртуальних активів та технологій штучного інтелекту (далі – ШІ).

«У 2022 році світова вартість кіберзлочинності оцінювалася приблизно в 8,4 трильйона доларів США. Вартість інцидентів, спричинених незаконною діяльністю в Інтернеті, у 2023 році перевищить позначку в 11 трильйонів доларів США. До 2026 року річні витрати на кіберзлочинність у всьому світі можуть перевищити 20 трильйонів, збільшившись майже на 150 відсотків порівняно з 2022 роком».

За оцінками Cybersecurity Ventures, якщо кіберзлочинність умовно розглядати як країну, то вона може бути оцінена як третя за розміром економіка світу після США та Китаю. «Це являє собою найбільшу передачу економічного багатства в історії, що ставить під загрозу стимули для інновації та інвестиції, експоненціально перевищує збиток, завданий стихійними лихами за рік, і буде прибутковішим, ніж світова торгівля всіма основними незаконними наркотиками разом узятими».

Подібний початок є традиційним для переважної більшості наукових текстів з питань протидії «комп'ютерним» злочинам. Такі міркування можна зустріти й у роботах авторів цього розділу монографії. Обрана нами скептична тональність не означає, що вони хибні. Вони правильні. Але на проблему «комп'ютерних» злочинів можна подивитися інакше.

Відповідно до даних офіційної статистики за останні десять років (2013 − 2022) кількість облікованих кримінальних правопорушень за Розділом XVI Особливої частини КК зросла від 595 до 3415, близькою є й динаміка скерованих до суду проваджень – від 259 до 2435. Натомість кількість відповідних судових рішень вимірюється числами іншого порядку і змінилася від 72 до 100 (Рис.1).

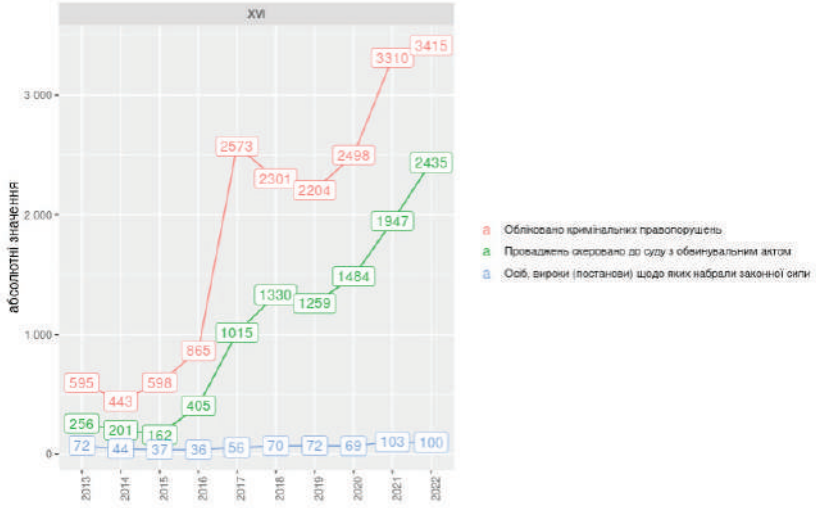

Рис. 1. Динаміка пов'язаних із правопорушеннями, передбаченими Розділом XVI Особливої частини КК: кількості облікованих проваджень, скерованих до суду проваджень та кількості осіб, судові рішення щодо яких набрали чинності

При цьому реальні покарання застосовувалися у 49% випадків (середній показник для всіх випадків засудження – 58%). Серед цих покарань у 75% призначався штраф, у 22% − позбавлення волі. Аналогічні показники для всіх покарань, призначених за період спостережень становлять: 39% − штраф, 36% − позбавлення волі.

Нарешті, частка проваджень, облікованих за статтями Розділу XVI серед всіх облікованих проваджень, становить від 0,1% у 2013 році до 0,9% у 2022 (1% у 2021). Частка осіб, засуджених за кримінальні правопорушення, передбачені статтями Розділу XVI, серед всіх засуджених складає від 0,04% у 2013 році, до 0,15% у 2022.

Такі «скромні» показники не відповідають згаданим раніше оцінкам небезпечності, заподіюваної «комп'ютерними» злочинами шкоди, поширеності цих посягань тощо. Водночас Україна обґрунтовано оцінюється як країна з достатнім високим рівнем інформатизації.

Приблизно 82% українців користуються інтернетом хоча б раз на тиждень, із них 78% щодня чи майже щодня. Такий рівень проникнення інтернету, за досвідом зарубіжних країн, істотно змінює сферу надання послуг, комунікацію громадян з державними органами і, на жаль, злочинність. Якщо перші напрями соціальної трансформації з усією очевидністю спостерігаються в Україні, то відповідної динаміки злочинності не виявлено. У чому проблема?

Зрозуміло, що відповідь на це питання не є простою та одномірною. Але спробуємо запропонувати основні, на нашу думку, підходи до раціонального пояснення встановленої невідповідності. Кримінально-правовий вплив на осіб, що вчинили діяння, передбачені Розділом XVI Особливої частини КК, характеризується в середньому рідшим застосуванням реальних покарань, в середньому частішим використанням більш м'яких покарань. Ми вважаємо, що це може свідчити про те, що у поле зору кримінальної юстиції потрапляють переважно найпростіші та найменш небезпечні форми відповідних кримінальних правопорушень. Таку проблему ми називаємо примітивізацією правозастосовчого рівня кримінально-правового регулювання. Так, за результатами дослідження судової практики по Розділу XVI Особливої частини КК у 2012 р. нами було зроблено такий висновок: практика національних судів містить рішення, у яких застосування кримінальної відповідальності до осіб, які вчиняли комп'ютерні злочини, було пов'язане з посяганнями, які дійсно є суспільно небезпечними (43,71%); разом із тим, більше половини судових рішень досліджуваної категорії (56,29%) пов'язані з кваліфікацією таких діянь, віднесення яких до суспільно небезпечних є досить спірним. Не виключаємо, що аналогічна проблема існує і зараз, можливо у дещо зміненому вигляді.

Тут варто звернути увагу на нещодавні зміни законодавства про кримінальну відповідальність.

Законом України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24.03.2022 р. №2149-IX було внесено зміни до Розділу XVI. Серед іншого було передбачено кримінальну відповідальність за вчинення несанкціонованого втручання

в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ч. 1 ст. 361), а також за вчинення таких дій у складі групи або повторно (ч. 2 ст. 361). Дії, які раніше вважалися основним складом кримінального правопорушення, передбаченого ч. 1 ст. 361, стали його особливо кваліфікованим складом (ч. 3 ст. 361) і отримали більш сувору санкцію. Ураховуючи визначені раніше ознаки примітивізації кримінально-правового регулювання в сфері інформаційної безпеки, здійснені зміни можуть стати причиною загострення названого негативного процесу.

Істотні трансформації відносин інформаційної безпеки в сфері використання інформаційних технологій, на нашу думку, будуть пов'язані із використанням *віртуальних активів* та поширенням технологій *ШІ*.

Поява технологій розподіленого зберігання даних (BlockChain) та заснованих на таких технологіях криптовалютних платіжних систем істотно змінює процес протидії злочинності. Трансформуються форми корупції, з'являються нові види неправомірної вигоди, оновлюються методи легалізації злочинних доходів, принципово змінюється фінансова складова незаконного обігу наркотиків, зброї тощо. Водночас як будь-який соціальний процес, *поширення криптовалюти* та технології BlockChain має діалектичні наслідки. З одного боку, криптовалюти стали новим інструментом злочинців. З іншого – наявність у відкритому доступі всієї бази даних транзакцій у системі криптовалюти дає правоохоронним органам принципово нові інструменти боротьби зі злочинністю[1].

За нашими оцінками, на вересень 2021 р. в Єдиному державному реєстрі судових рішень було обліковано 52 обвинувальних вироки, що стосувалися використання криптовалюти, 36 – використання криптовалюти для незаконного обігу наркотиків, 15 – «комп'ютерні» злочини, розповсюдження шкідливого програмного забезпечення для прихованого майнінга криптовалюти, продаж даних, 1 – шахрайство.

[1] Sedgwick K. Bitcoin is Great for Criminals. It's Even Better for Law Enforcement. *Bitcoin.com*: website. 16.07.2018. URL : https://news.bitcoin.com/bitcoin-is-great-for-criminals-its-even-better-for-law-enforcement/

У лютому 2023 р. реєстр містив вже 100 обвинувальних вироків: 59 – пов'язані з функціонуванням он-лайн мереж розповсюдження наркотиків (28 – «end users»), 19 – «комп'ютерні» злочини, 9 – посягання на власність, 5 – підробка документів, по 2 – незаконний обіг електронних грошей, збут порнографічних матеріалів, по 1 – злочини проти національної безпеки, легалізація доходів, незаконний обіг зброї, службовий злочин.

Очевидно, що така кількість судових рішень є вкрай незначною і сама по собі не може свідчити про істотний рівень використання криптовалюти злочинцями в Україні. Водночас очевидною є тенденція розширення злочинного використання віртуальних активів в Україні. Можна зазначити, що відбуваються як кількісні зміни – збільшення випадків злочинного використання віртуальних активів, так і якісні – збільшення видів злочинного використання віртуальних активів. До того ж, актуальні експертні дослідження свідчать, що рівень використання криптовалюти у національному сегменті злочинності є значним. Відповідно до The Chainalysis 2021 Crypto Crime Report[1] Україна посідала третє місце (після рф та США) за обсягом транзакцій на електронні гаманці, асоційовані з інтернет-магазинами наркотиків, які функціонують в darknet. Загальний обсяг транзакцій з України на гаманці інтернет-магазинів та з гаманців інтернет-магазинів в Україну склав у 2020 р. близько $100 млн.

Поза увагою міжнародних експертів не залишилося й прийняття в Україні Закону «Про віртуальні активи». Оглядачка Foreign Policy Елізабет Броу розмірковує про перспективи легалізації віртуальних активів в Україні та зазначає таке: «…до значного рівня корумпованості додається інструмент, який надає корупціонерам нові можливості … на кінець березня 2021 року українські державні службовці задекларували 46,351 біткоїнів, що складає близько $1.7 мільярда … Україна намагається отримати $2.2 мільярди від МВФ у 2021 році». Та підсумовує: «Велика ставка Києва на цифрові гроші може мати негативні наслідки і погіршити корупційні проблеми країни»[2].

[1] Grauer K., Updegrave H. The Chainalysis 2021 Crypto Crime Report. URL : https://go.chainalysis.com/2021-Crypto-Crime-Report.html

[2] Braw E. Ukraine Wants to Be Cryptocurrency Central. Foreign Poicy: website. URL : https://foreignpolicy.com/2021/06/02/ukraine-wants-to-be-cryptocurrency-central/

Враховуючи зазначене, вкрай важливою є мінімізація корупційних ризиків легалізації національного ринку криптовалют. Основними напрямами роботи тут мають стати: локалізація успішних практик правоохоронних органів, законодавче забезпечення та використання антикорупційного потенціалу BlockChain.

Нарешті, істотні зміни «комп'ютерної» злочинності пов'язують з розповсюдженням технологій *ШІ*[1]. Обґрунтованим є прогноз їх широкого використання для злочинних цілей[2]. Зокрема, вельми ймовірною є поява нових форм шахрайства на основі формування персонального інформаційного середовища та профілювання значної кількості людей із метою подальшого автоматизованого фішигу або вішингу. Ймовірними можуть стати масштабні кібератаки на основі автоматизованого виявлення уразливостей комп'ютерних систем та їх знову ж таки автоматизованого використання. Протиправне використання технологій ШІ можливе також шляхом створення високоякісних підробок відео- або аудіоконтенту, розробки надскладних схем легалізації доходів, здобутих злочинним шляхом тощо[3]. Ймовірною є поява принципово нових видів «комп'ютерних» кримінальних правопорушень. Ідеться про так звані «змагальні» атаки (adversarial attacks) та «отруєння» ШІ. Перші полягають у відшукуванні недосконалостей створених систем розпізнавання образів або мовлення (звуку) та подальшому їх використанні для приведення пристроїв зі ШІ у некоректний режим роботи. «Отруєння» ШІ полягає у втручанні в процес розробки пристроїв шляхом внесення змін до так званих «навчальних» наборів даних. У результаті подібних дій пристрій із ШІ у певних ситуаціях функціонує у спосіб, який значно відрізняється від запланованого розробниками[4].

---

[1] Карчевський М. В. Штучний інтелект та протидія злочинності. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право. 2020. 112 с

[2] Dupont B., Stevens Y., Westermann H., Joyce M. Artificial Intelligence in the Context of Crime and Criminal Justice. Korean Institute of Criminology, Canada Research Chair in Cybersecurity, ICCC, Université de Montréal. 2018. Pp. 33–37. URL: https://www.cicc-iccc.org/public/media/files/prod/publication/files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf.

[3] Там само. С. 40–56.

[4] Там само. С. 58–60.

1.1.3. Основні проблеми кримінально-правової охорони відносин інформаційної безпеки в сфері забезпечення доступу до інформації та в сфері формування інформаційного ресурсу

Проблеми кримінально-правової охорони відносин інформаційної безпеки *в сфері забезпечення доступу до інформації* стосуються головним чином розбалансованості законодавства, існуванні численних конкуруючих норм, надмірного рівня кількості кримінально-правових заборон у цій сфері. Необхідною є оптимізація означеної системи норм, заміни наявної розосередженої системи спеціальних кримінально-правових заборон такими, які б забезпечували регулювання більш широких сегментів інформаційної безпеки.

Основне питання кримінально-правової охорони відносин інформаційної безпеки *в сфері формування інформаційного ресурсу* полягає у чіткому та послідовному визначенні межі можливостей ефективного впливу на суспільні відносини засобами кримінального права. У суспільно-політичному дискурсі, у науці небезпеки інформаційних впливів та зловживань обговорюються достатньо широко. Багатомірність та масштабність шкоди від неконтрольованого інформаційного простору не викликає сумнівів. Разом з цим розв'язання означених проблем шляхом доповнення КК новими нормами навряд чи є доцільним. Неодноразово пропонувалося встановлювати покарання за різноманітні форми маніпуляції суспільною свідомістю. Такі пропозиції є спірними через прогнозовану неефективність і декларативність, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації. Крім того, поширення глобальних інформаційних технологій взагалі робить методи обмеження або заборони контенту все менш ефективними. Яскравим прикладом тут може слугувати відомий «ефект Стрейзанд». Розв'язання проблеми знаходиться поза межами кримінально-правового регулювання і, на нашу

думку, передбачає передусім системну роботу в системі освіти та формуванні конкурентних інформаційних продуктів.

В означеному контексті неможливо не звернути уваги на доповнення КК України новими заборонами у 2022 році. Однією з таких заборон була стаття 436[2] КК, що передбачила відповідальність за виправдовування, визнання правомірною, заперечення збройної агресії російської федерації проти України, глорифікацію її учасників. КК доповнено статтею 436[2] згідно із Законом № 2110-IX від 03.03.2022 р. У 2022 році за ознаками цього правопорушення було обліковано 1354 провадження, засуджено 200 осіб. Відповідно до пояснювальної записки, мета доповнення КК ст. 436[2] КК визначалася як протидія засобами кримінально-правового впливу ворожим інформаційним впливам в умовах триваючої гібридної війни рф з Україною. Прогноз соціально-економічних та інших результатів прийняття проєкту передбачав посилення ефективної протидії гібридній інформаційній війні, що її веде держава-агресор проти України, захист державного суверенітету та територіальної цілісності України, зміцнення патріотичних настроїв у ЗСУ та загалом в українському суспільстві[1].

Нами проведено дослідження того, наскільки отримані результати її застосування наближені до прогнозованих. Розглянемо показники протидії кримінальному правопорушенню, передбаченому ст. 436[2] КК, у контексті аналогічних середніх даних, даних, що характеризують застосування всіх норм КК протягом останніх 10 років (2013–2022).

По-перше, як правило (середнє значення), суди призначають реальне покарання 58% осіб, визнаних винними у вчиненні кримінальних правопорушень, 42% визнаних винними осіб звільняються від покарання. Лише 15% осіб, визнаних винними у вчиненні криміналь-

[1] Проект Закону про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції). Номер, дата реєстрації: 5102 від 18.02.2021. *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5102&conv=9

них правопорушень, передбачених ст. 436[2] КК, отримали за рішеннями національних судів реальні покарання (85% винних осіб було звільнено від покарання).

По-друге, істотно відрізняється від середніх значень віковий розподіл осіб, визнаних винними у вчиненні кримінальних правопорушень, передбачених ст. 436[2] КК. 27% − від 30 до 50 років (середнє значення 49%), 44% − від 50 до 65 років (середнє значення 10%), 25%(!) – від 65 років (середнє значення 1%).

По-третє, серед осіб, визнаних винними у кримінальних правопорушеннях, передбачених ст. 436[2] КК, 48% працездатних осіб, які на момент вчинення правопорушення не працювали (середнє значення 72%), та 35% пенсіонерів (середнє значення 10%).

По-четверте, розподіл засуджених в Україні за останні 10 років за рівнем освіти був таким: 7% – повна вища освіта, 23% – професійнотехнічна, 40% – повна загальна середня, 25% – базова загальна середня. Цей розподіл істотно відрізняється для осіб, засуджених за вчинення кримінальних правопорушень, передбачених ст. 436[2] КК 26% – вища освіта, 22% – повна загальна середня.

По-п'яте, за вчинення кримінального правопорушення, передбаченого ст. 436[2] КК, у складі групи у 2022 році не засуджено жодну особу. Серед всіх засуджених частка засуджених за вчинення правопорушень у складі групи складає близько 13%.

По-шосте, середня частка жінок серед засуджених складає 12%. Середня частка жінок серед засуджених за ст. 436[2] КК – 34%.

По-сьоме, більшість рішень про засудження осіб, за кримінальні правопорушення, передбачені ст. 436[2] КК, приймаються судами, що розташовані у областях, які межують з районами бойових дій.

Наведені дані, на нашу думку, свідчать, що задекларовані цілі доповнення КК України ст. 436[2] не досягнуто. Рівень застосування звільнення від покарання свідчить, що скоріше за все у судах у переважній більшості опиняються справи щодо обвинувачення у наймеш небезпечних проявах глорифікації. Це додатково підтверджується аномальними, у контексті загальних показників протидії злочинності, даними, що характеризують вік, стать, освіту та заняття засуджених

за вчинення кримінальних правопорушень, передбачених ст. 436[2] КК України. Можна стверджувати, що спостерігається примітивізація кримінально-правової протидії виправдовуванню, визнанню правомірною, запереченню збройної агресії рф проти України, глорифікації її учасників.

Необхідність ефективного кримінально-правового регулювання в умовах протидії військовій агресії рф та в процесі відновлення після перемоги над агресором є очевидною. Невідповідність цілей та прогнозів соціальних ефектів криміналізації тенденціям практичного кримінально-правового регулювання потребує розгляду проблеми в контексті прагматичної парадигми кримінального права та підтверджує висловлені зауваження щодо необхідності визначення меж ефективного кримінально-правового впливу на відносини інформаційної безпеки в сфері формування інформаційного ресурсу. Крім того, наявний досвід вкотре актуалізує проблематику нечітких формулювань заборон та необхідності законодавчої визначеності.

Таким чином, інформаційну безпеку будемо розглядати як систему суспільних відносин щодо забезпечення реалізації інформаційної потреби громадян, суспільства, держави. Структуру інформаційної безпеки складають відносини в сфері використання інформаційних технологій, відносини в сфері забезпечення доступу до інформації та відносини в сфері формування інформаційного ресурсу. Кожному з названих елементів інформаційної безпеки властиві специфічні проблеми кримінально-правової охорони. Для використання інформаційних технологій це примітивізація та неготовність до використання новітніх технологій зі злочинною метою. Для забезпечення доступу до інформації – надмірна розгалуженість та неузгодженість заборон. Для формування інформаційного ресурсу – визначення меж кримінально-правового впливу. Друга означена проблема, як видається, має локальний характер, її ефективне розв'язання цілком можливе в межах національного правового дискурсу. Водночас розв'язання першої та третьої потребують аналізу наявного зарубіжного та міжнародного досвіду.

1.2. Міжнародні стандарти та досвід протидії кримінальним правопорушенням в сфері використання інформаційних технологій

Проблема дослідження питань, пов'язаних із кіберзлочинністю, є надзвичайно важливою і актуальною, це обумовлено декількома чинниками: по-перше, це особлива сфера застосування – мережа «Інтернет», по-друге, Україна обравши курс євроінтеграції, повинна привести своє законодавство у відповідність. Тобто ми говоримо про процес гармонізації та адаптації українського законодавства до європейського і активну протидію кіберзлочинності як проблемі транснаціонального характеру.

На важливість боротьби з кіберзлочинністю, зокрема, вказується у п. 2.2 Плану дій Ради Європи для України «Стійкість, відновлення та відбудова» 2023–2026 р., де зазначається, що його метою є надання підтримки органам державної влади України в частині оцінювання, зменшення та управління ризиками економічної злочинності, включно з ризиками, пов'язаними з корупцією, відмиванням грошей та фінансуванням тероризму, кіберзлочинністю, електронними доказами та доказами, що мають транскордонне значення, зважаючи на ослаблені інститути й структури управління, низьку здатність освоєння коштів і масові потоки зовнішньої фінансової допомоги, в контексті діяльності із відновлення і заходів, що сприяють поверненню переміщених осіб[1].

Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. №2163-VIII у ст. 1 визначається поняття кіберзлочинність як сукупність кіберзлочинів та відповідно кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке

[1] План дій Ради Європи для України «Стійкість, відновлення та відбудова» 2023–2026 р. https://rm.coe.int/action-plan-ukraine-2023–2026-ukr/1680aa8282

передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України[1].

У межах нашого дослідження здійснимо аналіз міжнародних стандартів, рекомендацій ЄС щодо протидії «кіберзлочинам». Зокрема, Конвенції Ради Європи про кіберзлочинність від 23.11.2001 р.[2] та Директиви Європейського парламенту і ради ЄС 2016/1148 від 06.07.2016 р. про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу.[3]

Так, 23 листопада 2001 року Радою Європи була прийнята Конвенція про кіберзлочинність, яка була ратифікована Україною 07.09.2005 р. (далі – Конвенція), з Додатковим протоколом до неї, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р., що набрав чинності для України 01.04.2007 р.[4].

У II розділі Конвенції визначено заходи, що мають здійснюватися на національному рівні, і вказано на чотири групи правопорушень: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерами; 3) правопорушення, пов'язані зі змістом, 4) правопорушення, пов'язані з порушенням авторських та суміжних прав[5].

---

[1] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. №2163-VIII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

[2] Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

[3] Директива Європейського парламенту і ради ЄС 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу від 06.07.2016 р. №2016/1148. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

[4] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Міжнародний документ від 28.01.2003 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text

[5] Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

Із аналізу Конвенції зрозуміло, що визначаються конкретні кримінальні правопорушення, які необхідно гармонізувати із законодавством держав-членів, що її ратифікували з метою спільної боротьби з кіберзлочинністю.

Варто вказати, що використана у Конвенції про кіберзлочинність класифікація відповідних злочинів теж не є досконалою, адже групи виділяються за різними критеріями. Однак, попри всі недоліки важливість цього документа є беззаперечною, а належну імплементацію його положень у національне законодавство віднесено до основних рекомендацій державам за результатами дослідження Європолу у 2016 році[1].

Зазначимо, що порівняльний аналіз Конвенції та КК України дає можливість установити, що більшість діянь, передбачених у Конвенції, визнаються в українському законодавстві кримінальними правопорушеннями. До таких діянь належать: нелегальне перехоплення (ст. ст. 163, 361, 362 КК); навмисний доступ (ст. 361 КК), втручання в дані (ст. ст. 361, 362 КК); втручання в систему (ст. 361 КК); злочини, пов'язані з дитячою порнографією (ст. 301 КК); підробка, пов'язана з комп'ютерами (ст. ст. 358, 366 КК); шахрайство, пов'язане з комп'ютерами (ч. 3 ст. 190 КК). Діяння, передбачені Додатковим протоколом до Конвенції, охоплюються ст. 161 КК, яка встановлює відповідальність за порушення рівноправності громадян залежно від їх расової, національної належності або ставлення до релігії, та загальними нормами Особливої частини КК України, що передбачають злочини проти свободи совісті (ст. 178–181 КК)[2]. Також до цього переліку можна додати склади кримінальних правопорушень, що передбачені ст. 361[2] КК України («Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електро-

[1] Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. С. 26, 27. URL: https://doi.org/10.32837/11300.26072

[2] Карчевський М. В. Кримінально-правова охорона інформаційної без- пеки України : монограф. МВС Ук- раїни, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка.Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 260, 261.

нно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації») та ст. 361[1] КК України («Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»).

Досліджуючи Конвенцію, маємо також зауважити, що національне кримінальне законодавство прямо не передбачає відповідальності за такі дії, як:

1) навмисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст.ст. 2–5 Конвенції;

2) володіння пристроями, включаючи комп'ютерні програми, створені або адаптовані насамперед з метою вчинення будь-якого зі злочинів, перелічених у ст.ст. 2–5 Конвенції, або комп'ютерними паролями, кодами доступу або подібними даними, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2–5 Конвенції, з наміром використання зазначених пред- метів для вчинення будь-якого зі злочинів, перерахованих у ст.ст. 2–5[1].

Однак, видається, що законодавство України про кримінальну відповідальність містить достатньо засобів кримінально-правової охорони від посягань, які вчиняються у співучасті, а також засобів протидії попередній злочинній діяльності. Так, ураховуючи визначення Конвенції, конститутивною ознакою яких є мета подальшого вчинення злочинів, навмисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних являють собою пособництво у вчиненні відповідних злочинів. У свою чергу, володіння шкідливими засобами з метою подальшого вчинення злочинів необхідно, відповідно до на-

[1] Карчевський М. В. Кримінально-правова охорона інформаційної без- пеки України : монограф. МВС Ук- раїни, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка.Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 263–264

ціонального законодавства, уважати готуванням. Як бачимо з наведених вище визначень, Конвенція пропонує встановлювати кримінальну відповідальність не просто за володіння, розповсюдження або придбання шкідливих програмних чи технічних засобів, кодів доступу чи іншої подібної інформації, а лише в тому випадку, коли ці дії вчиняються з метою подальшого скоєння комп'ютерних злочинів. Таким чином, Конвенція, на нашу думку, містить достатньо вдале формулювання, що чітко відображає суспільну небезпечність діянь, пов'язаних зі шкідливими програмними чи технічними даними[1].

Значний інтерес становить також дослідження Закону України «Про ратифікацію Конвенції про кіберзлочинність» № 2824-IV від 07.09.2005 р. У ньому зазначається про ратифікацію Конвенції про кіберзлочинність з такими застереженнями і заявами:

до п. 1 ст. 6:

Україна залишає за собою право не застосовувати п. 1 ст. 6 Конвенції в частині встановлення кримінальної відповідальності за виготовлення, придбання для використання, надання для використання іншим чином предметів, зазначених у підпункті 1.a.i, та виготовлення і придбання для використання предметів, зазначених у підпункті 1.a.ii ст. 6 Конвенції;

до п. 1 ст. 9:

Україна залишає за собою право не застосовувати повністю підпункти 1.d та 1.e ст. 9 Конвенції[2]. Як видається, у цьому законі також містяться недоліки, пов'язані з неадекватним відображенням реального змісту суспільної небезпечності досліджуваних посягань. Так, Конвенція формулює типові ознаки складів комп'ютерних злочинів та пропонує механізм так званих застережень, який дозволяє максимально враховувати особливості національного розуміння понять «злочин» та «суспільна небезпечність» на рівні законодавств окремих

[1] Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2824–15#Text

[2] Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монограф. МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка.Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 267.

держав. Україна використовує цей механізм для того, щоб відмовитися від криміналізації:

1) виготовлення, придбання для використання, надання для використання іншим чином пристроїв, включаючи комп'ютерні програми, створені або адаптовані насамперед із метою вчинення будь-якого зі злочинів, перерахованих у ст.ст. 2–5 Конвенції;

2) виготовлення і придбання для використання комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст.ст. 2–5 Конвенції;

3) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації.

На цьому перелік застережень закінчується. І це фактично призводить до того, що Україна бере на себе зобов'язання визнавати кримінальними правопорушеннями діяння, які характеризуються недостатньою суспільною небезпечністю. Наприклад, у п. 1 ст. 4 Конвенції пропонується встановлювати відповідальність за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це. Україною ця норма ратифікована без застережень. Саме про це йдеться у ч. 3 ст. 361 чинної редакції КК, яка передбачає відповідальність за несанкціоноване втручання в роботу комп'ютерних систем, що призвело до втрати, підробки, блокування інформації блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації[1].

Погоджуємося з М. І. Хавронюком, який зазначає, що наслідки у виді «витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації», що були передбачені в ч. 1 ст. 361 КК, з цієї частини виключені і визначені у новій ч. 3 ст. 361 КК. При цьо-

[1] Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монограф. МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка.Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 264, 265.

му злочин, передбачений ч. 1 ст. 361 КК, який карався, зокрема, позбавленням волі на строк до трьох років, трансформовано у кримінальний проступок. Тут має місце помилка законодавця – надмірна криміналізація. Так, саме по собі несанкціоноване втручання в роботу згаданих систем чи мереж не є кримінальним правопорушенням, оскільки не створює жодних наслідків, що можна було б охопити поняттям істотної шкоди (див. ст. 11 КК)[1].

Так, у Вироку Снятинського районного суду Івано-Франківської області від 12.02.2013 р. зазначено, що підсудний не маючи договорів з власниками телерадіопрограм чи їх дистрибюторами про прийом і подальше розповсюдження кодованих супутникових телевізійних каналів на території України та не отримавши кодів чи картки доступу до вказаних каналів, розкодував приймач супутникових телевізійних каналів моделі «4100С» з індивідуальним серійним номером 120400364, ввівши в нього спеціальні коди доступу українських телевізійних каналів супутникового телебачення. Таким чином своїми умисними діями, які виразились в несанкціонованому втручанні в роботу мереж електрозв'язку, що призвело до витоку інформації ОСОБА_1 вчинив злочин, передбачений ст. 361 ч. 1 КК України[2]. Також у Вироку Ленінського районного суду м. Запоріжжя від 04.09.2020 р. зазначено, що Особа_4, маючи умисел на несанкціоноване втручання в мережу електрозв'язку з подальшим розповсюдженням інформації з обмеженим доступом, встановив супутникове обладнання, налаштувавши цифровий ресивер супутникового телебачення моделі «Sat Integral1228», підключив останній до всесвітньої мережі Інтернет, приєднав до телевізору, тим самим надав можливість відтворення каналів «Футбол 1» та «Футбол 2», що передаються

[1] Хавронюк М. І. Аналіз Закону «щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» із серії науково-практичних коментарів Миколи Хавронюка про зміни до Кримінального кодексу, прийняті під час воєнного стану. *Центр політико-правових реформ*: вебсайт. URL: https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist/

[2] Вирок Снятинського районного суду Івано-Франківської області від 12 лютого 2013 року. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: https://reyestr.court.gov.ua/Review/31776005

в мережі кабельного телебачення та є інформацією з обмеженим доступом, котра належить компанії ТОВ «ТРК Україна»[1].

Подібні зауваження стосуються і невикористання Україною можливостей ратифікації із застереженнями, що містяться в ст. ст. 2, 3, 7 Конвенції. Так, криміналізація незаконного доступу (ст. 2) можлива із застереженням, що стосується мети подібних дій. У документі зазначається, що сторона може вимагати, щоб таке правопорушення було вчинено з недобросовісною метою. Отже, доречніше було б приєднатися до цієї частини Конвенції саме з таким застереженням, яке пропонується, але Україною не використане. Застереження щодо мети наявні і в нормах Конвенції щодо кримінальної відповідальності за нелегальне перехоплення (ст. 3) та підробку, пов'язану з комп'ютерами (ст. 7). Їх використання є необхідним для приведення зобов'язань, узятих на себе Україною у сфері гармонізації кримінального законодавства, у відповідність до реальних потреб суспільства та національних особливостей кримінальної правотворчості[2].

Сьогодні кримінальне законодавство України зіткнулося з реальною загрозою його неконтрольованого і безсистемного реформування, результатом чого цілком може стати не лише подальше його «захаращення» науково необґрунтованими і такими, що не викликані потребами сучасного суспільного життя положеннями, а й, зрештою, може призвести до порушення основоположних принципів, на яких воно побудоване, системних зв'язків і залежностей його приписів, що у свою чергу потягне за собою істотне зниження ефективності засобів кримінально-правового впливу на злочинність[3]. У контексті цього зазначимо, що норми у цій сфері достатньо криміналізовано

---

[1] Вирок Ленінський районний суд м. Запоріжжя від 04 вересня 2020 року. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: https://reyestr.court.gov.ua/Review/91433712

[2] Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монограф. МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка.Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 266

[3] Тацій В., Тютюгін В., Пономаренко Ю. Проблеми стабільності й динамізму кримінального законодавства України на сучасному етапі. *Вісник Національної академії правових наук України*. 2015. №4 (83). С. 64

і основною у напряму його удосконалення має бути саме робота над застереженнями.

Перейдемо до дослідження Директиви Європейського парламенту і ради ЄС 2016/1148 від 06.07.2016 р. про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу[1]. Проаналізувавши текст, можемо зазначити, що у Директиві вказується про мережеві та інформаційні системи. Відповідно до ст. 1 ця Директива встановлює інструменти, маючи на меті досягти високого спільного рівня безпеки мережевих та інформаційних систем в межах Союзу для того, щоб покращити функціонування внутрішнього ринку. З цією метою ця Директива: (a) встановлює обов'язки для всіх держав-членів для ухвалення національної стратегії безпеки мережевих та інформаційних систем; (b) створює Групу співпраці для підтримки та сприяння стратегічній співпраці та обміну інформацією серед держав-членів та розвитку повної довіри між ними; (c) створює мережу груп реагування на інциденти, пов'язані з комп'ютерною безпекою («мережа CSIRT») з метою зміцнення повної довіри між державами-членами та сприяння швидкій та дієвій оперативній взаємодії; (d) встановлює вимоги до безпеки та повідомлення для операторів основних послуг та надавачів цифрових послуг; (e) встановлює обов'язки для держав-членів для призначення національних компетентних органів, єдиних контактних пунктів та CSIRT із завданнями, пов'язаними з безпекою мережевих та інформаційних систем. Також вказується, що ця Директива не обмежує дій, що їх вживають держави-члени для охорони своїх істотних державних функцій, зокрема для забезпечення національної безпеки, у тому числі дій щодо захисту інформації, розкриття якої держави-члени вважають таким, що суперечить суттєвим інтересам їхньої безпеки, та для підтримки закону та порядку, зокрема щоби уможливити розслідування, розкриття та кримінальне переслідування кримінальних

[1] Директива Європейського парламенту і ради ЄС 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу від 06.07.2016 р. №2016/1148. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

правопорушень. Директива NIS є першим інструментом внутрішнього ринку, спрямованим на підвищення опірності ЄС до ризиків у сфері кібербезпеки. Вона орієнтована на забезпечення безперервності послуг, що дають економіці та суспільству ЄС змогу функціонувати належним чином. З цією метою Директива NIS запроваджує конкретні заходи з розбудови можливостей кібербезпеки в ЄС та зменшення зростаючих загроз для мережевих та інформаційних систем, які використовуються для надання основних послуг у ключових секторах[1].

Про важливість цієї Директиви вказується також у Указі Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію кібербезпеки України» зазначається, що для досягнення цілі В. 3 Україна розвиватиме міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України, шляхом: продовження співробітництва з Агентством Європейського Союзу з питань мережевої та інформаційної безпеки, зокрема з питань скоординованого розкриття вразливостей та імплементації Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 06.07.2016 р. про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу як елементу євроінтеграції України[2].

Специфіка ще одної складової визначеної нами раніше проблеми кримінально-правового регулювання в сфері використання інформаційних технологій – *протидії злочинному використанню віртуальних активів* – полягає у тому, що в Україні в умовах незавершеності правового регулювання використання віртуальних активів (прийнято відповідний закон, але він набере чинності після внесення змін до Податкового кодексу), спостерігається фактичне використання віртуаль-

[1] Комітет з питань цифрової трансформації. Норми законодавства Європейського Союзу, які необхідно впровадити в проєкти законів про кібербезпеку та про об'єкти критичної інфраструктури в Україні: аналітичний звіт. С. 19 URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_03.pdf

[2] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021. *Офіс Президента України*: оф. вебсайт. URL: https://www.president.gov.ua/documents/4472021–40013

них активів для вчинення кримінальних правопорушень. Раніше ми наводили результати відповідного аналізу реєстру судових рішень.

У зв'язку з цим, певний інтерес представляють собою міжнародні ініціативи протидії так званій «криптозлочинності». Однією з таких є щорічна конференція Робочої групи з протидії злочинному використанню фінансів і криптовалют, яка є тристоронньою ініціативою Базельського інституту урядування, Інтерполу та Європолу[1]. Рекомендації цих конференцій представляють собою зріз найбільш актуальних проблем протидії злочинному використанню віртуальних активів та безсумнівно є важливими для побудови відповідної системи в Україні.

Так, рекомендації конференції 2021 року[2] фокусують увагу на таких аспектах організації протидії злочинному використанню віртуальних активів:

1. Міжнародне співробітництво. Усвідомлюючи гіперглобальність індустрії віртуальних активів, відзначається необхідність прискорення обміну інформацією між правоохоронними органами, важливість обміну ресурсами, новими розробками, призначеними для розслідування фактів злочинного використання віртуальних активів.

2. Викриття віртуальних активів. Брак правового регулювання віртуальних активів приводить до втрати національними правоохоронними органами можливості протидіяти «криптозлочинності», виявляти незаконні фінансові потоки. Оскільки кількість незаконних активів, які зберігаються у вигляді криптовалют, зростає, ця неспроможність ставатиме все більшою перешкодою для зусиль країн у боротьбі з фінансовими злочинами.

3. Державно-приватне партнерство. Необхідність довіри та ефективних механізмів співпраці між державним і приватним секторами для боротьби з відмиванням грошей у вигляді віртуальних активів.

---

[1] 7th Global Conference on Criminal Finances and Cryptocurrencies. *Basel Institute on Governance*: website. URL: https://baselgovernance.org/node/2446

[2] Recommendations of the Tripartite Working Group on Criminal Finances and Cryptocurrencies on Combating virtual assets-based money laundering and crypto-enabled crime. *Basel Institute on Governance*: website. URL: https://baselgovernance.org/publications/combating-virtual-assets-based-money-laundering-and-crypto-enabled-crime

4. Необхідість міжнародної гармонізації нормативного регулювання віртуальних активів.

5. Важливість постійного вдосконалення діяльності правоохоронних органів, їх технічної оснащеності, актуалізації професійних знань та навичок.

Крім підтвердження значення державно-приватного партнерства та розвитку можливостей правоохоронних органів протидіяти злочинному використанню віртуальних активів, рекомендації конференції 2022 року[1] починаються з положення про те, що необхідно усунути бар'єри між традиційною та «криптозлочинністю». Йдеться про те, що подальше проникнення віртуальних активів до сфер, де зазвичай використовувалися традиційні фінанси властиве й злочинній діяльності, зокрема відмиванню коштів. У такій обстановці пропонується обмежити практику створення спеціалізованих підрозділів правоохоронних органів як неефективну. Як більш раціональний підхід розглядається включення фахівців зі знаннями в сфері віртуальних активів до підрозділів, що здійснюють протидію традиційній злочинності.

При розробці нового законодавства про фінансові злочини або перегляді існуючих законів пропонується використовувати достатньо широкі формулювання, щоб охоплювати як віртуальні активи, так і можливі майбутні зміни криптоіндустрії. Такий підхід забезпечить подолання давно відомої проблеми «хронічного відставання кримінального законодавства», проблеми невідповідності законодавства формам та способам злочинної діяльності в сфері використання технологій.

Як можна побачити, криміногенний вплив появи та розширення сфери застосування віртуальних активів розглядається як такий, що в меншій мірі потребує змін кримінального законодавства, але актуалізує завдання правового регулювання обігу віртуальних активів на національному рівні. Крім того важливою проблемою визнається

[1] Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering. *Basel Institute on Governance*: website. URL: https://baselgovernance.org/publications/seizing-opportunity-5-recommendations-crypto-assets-related-crime-and-money-laundering

організаційно-технічний рівень готовності правоохоронних органів протидіяти злочинному використанню віртуальних активів.

ШІ та протидія злочинності. За нашою оцінкою сучасний рівень розвитку технологій ШІ не потребує оновлення кримінального законодавства. Водночас активне використання цих технологій правоохоронними та судовими органами, а також істотні трансформації правового регулювання інформаційної приватності потребують розгляду питань правового регулювання ШІ в контексті досліджуваних нами питань.

За останні двадцять років ШІ пройшов шлях від наукової абстракції та концептуальних моделей до практичних задач та повсякденного використання. Системи ШІ використовуються практично в усіх сферах діяльності людини. Відбулися зміни у науковій рефлексії та правовому регулюванні соціалізації ШІ.

Збройна агресія рф прискорила практичне впровадження технологій ШІ в роботу національних правоохоронних органів. Розслідування воєнних злочинів, діяльності колаборантів, пропаганди на користь агресора вимагають оперативного опрацювання значних масивів даних. Правоохоронні органи активно використовують системи розпізнавання обличчя, відеоаналітику, транскрибування відео та аудіозаписів. Водночас *використання ШІ правоохоронними органами без належного правового регулювання та комплексу організаційно-технічних заходів для дотримання нормативних приписів може привести до системних порушень прав людини, та, як наслідок, ускладнити євроінтеграційні процеси, діалог із міжнародними партнерами України*. Тому дослідження цієї теми вбачається вкрай актуальним.

Експерти визначають чотири загальні групи ризиків[1] використання технологій ШІ. Проблеми їх мінімізації переважно складають зміст актуальної наукової дискусії щодо соціалізації технологій ШІ.

[1] Dupont B., Stevens Y., Westermann H., Joyce M. Artificial Intelligence in the Context of Crime and Criminal Justice: a report for the Korean Institute of Criminology. Canada Research Chair in Cybersecurity International Centre for Comparative Criminology – Université de Montréal. 2018. 228 p. URL: https://www.cicc-iccc.org/public/media/files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf

Нова якість порушення таємниці приватного життя. Автоматизована обробка даних про людину створює новий рівень загроз для людини. Аналіз уподобань у соціальних мережах[1], історії покупок[2], інтернет-з'єднань[3] з використанням технологій ШІ здатен більш ніж істотно порушити таємницю приватного життя конкретної людини.

Маніпулювання поведінкою. Технології ШІ вже сьогодні чинять істотний вплив на поведінку споживачів шляхом таргетованої реклами, індивідуалізованих рекомендацій пошукових сервісів, персоналізованих стрічок новин тощо. Значною є небезпека маніпуляцій з використанням ШІ у політичній діяльності[4]. Існує навіть спеціальний термін − «астротурфінг»[5], яким позначають імітацію громадської підтримки ініціатив[6].

---

[1] Kosinski M., Stillwell D., Graepel T. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences.* 2013. №110(15). Pp. 5802–5805. URL: http://dx.doi.org/10.1073/pnas.1218772110

[2] Hill K. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. 2012. *Forbes*: website. URL: www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

[3] Zalnieriute M. Big Brother Watch and Others v. the United Kingdom. *American Journal of International Law.* 2022. №116(3). Pp. 585–592. URL: http://dx.doi.org/10.1017/ajil.2022.35

[4] Yuval Noah. Harari argues that AI has hacked the operating system of human civilisation. 2023. *The Economist*: website. URL: www.economist.com/by-invitation/2023/04/28/yuval-noah-harari-argues-that-ai-has-hacked-the-operating-system-of-human-civilisation; Guggenberger N., Salib P. From Fake News to Fake Views: New Challenges Posed by ChatGPT-Like AI. 2023. *Default*: website. URL: www.lawfaremedia.org/article/fake-news-fake-views-new-challenges-posed-chatgpt-ai

[5] Grassroots (з англ. – «коріння трави») – термін сучасної американської політології; так у США називають спонтанні руху «знизу». Під grassroots розуміються умовно кажучи «справжні» рухи, організовані громадянами для боротьби за свої права. Імітацію ж «кореневого руху» називають astroturfing; у цьому випадку за псевдонародним рухом є політичне лобі (Grassroots. 2004. *Wikipedia*: website. URL: https://en.wikipedia.org/wiki/Grassroots)

[6] Dupont B., Stevens Y., Westermann H., Joyce M. Artificial Intelligence in the Context of Crime and Criminal Justice: a report for the Korean Institute of Criminology. Canada Research Chair in Cybersecurity International Centre for Comparative Criminology – Université de Montréal. 2018. 228 p. URL: https://www.cicc-iccc.org/public/media/files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf

Дискримінація. Через особливості машинного навчання технології, яка лежить в основі ШІ, недостатня якість даних, використаних в процесі розробки системи, може призвести до системних порушень її функціонування. Прикладом означеної проблеми може слугувати упередженість автоматизованих систем відбору персоналу. «Навчальний» набір даних для таких систем як правило представляє собою відомості щодо успішних рішень з підбору персоналу. Оскільки цей процес у багатьох сферах не є гендернонейтральним, мали місце випадки уведення в експлуатацію систем, що помножували гендрену нерівність під час функціонування[1].

Непрозорість. Правові гарантії інтелектуальної власності та конкурентна боротьба на ринку інформаційних технологій зумовлюють закритість алгоритмів систем ШІ, що унеможливлює перевірку правильності рішень та ефективний контроль за їх станом. У тих сферах де неправильна робота систем ШІ здатна заподіяти значну шкоду, така ситуація створює небезпеку.

Означені ризики досить чітко окреслюють проблеми застосування систем ШІ для протидії злочинності. Використання систем ШІ правоохоронними та судовими органами здатне забезпечити якісне оновлення їх діяльності. У зарубіжних країнах у практику правоохоронних органів впроваджені проєкти, пов'язані із класифікацією та розпізнаванням об'єктів, розпізнаванням звукових сигналів (мови або, наприклад, системи визначення пострілів). Запропоновані технічні рішення для аналізу великих об'ємів даних на основі алгоритмів машинного навчання. У такий спосіб здійснюється аналіз відомостей про телефонні або інтернет-з'єднання, про використання платіжних систем, віртуальних активів тощо. Такі рішення використовуються як потужні інструменти розслідування злочинів. Розробляються системи прогнозування злочинності та оцінки ризику індивідуальної протиправної поведінки на основі ШІ.

Водночас ризики використання таких систем не обмежуються небезпекою порушень таємниці приватного життя. Значними є ризи-

[1] 5 Examples of Biased Artificial Intelligence. 2019. *Misinformation-Fighting, AI-powered News & Fact Checking*: website. URL: www.logically.ai/articles/5-examples-of-biased-ai

ки дискримінації та непрозорості. Алгоритми оцінки кримінального ризику (criminal risk assessment algorithms) використовуються деякими судами для прийняття рішень щодо визначення виду покарання, доцільності перебування у в'язниці до суду, суворості вироків. Теоретично це зменшує упередженість, оскільки судді приймають рішення на основі обробки даних, а не власних, можливо, суб'єктивних, переконань. При цьому постає надзвичайно важливе питання. Через те, що базою для алгоритму є прийняті раніше рішення, він (алгоритм) може посилювати й увічнювати упередження, генерувати ще більшу кількість упереджених даних для подальших циклів ще більш упереджених рішень[1]. Наприклад, якщо перед суддею особа з невеликим доходом, алгоритм з дуже великою ймовірністю буде радити застосувати ув'язнення до суду. Наступного разу в подібній ситуації алгоритм буде ще категоричніший, наступного – ще й ще…

Подібні проблеми існують і під час впровадження систем прогнозування злочинності[2]. Ідея полягає в тому, що на підставі аналізу даних про зареєстровані кримінальні правопорушення системи визначають райони, що потребують посиленої уваги правоохоронних органів. У ці райони направляється більша кількість патрулів, чим має забезпечуватися більш ефективне використання ресурсів та досягатися необхідний рівень безпеки громадян. Результати впровадження таких системи показали зворотній бік проблеми. Чим більше поліцейських направлялося у заданий район, тим більшою була кількість виявлених у цьому районі правопорушень. Алгоритм фіксував прийняте рішення як правильне і продовжував рекомендувати посилені наряди для визначених районів. У такий спосіб увічнювався «кримінальний» статус таких районів, але загальне використання ресурсів поліції не ставало більш ефективним, загальний рівень безпеки громадян не підвищувався.

Наприклад, щоб оцінити упередженість поліцейського прогнозування, Група аналізу даних з прав людини (HRDAG) проаналізувала

[1] Hao K. AI is sending people to jail – and getting it wrong. 2019. *MIT Technology Review* website. URL: www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/

[2] Trejo O. What Is Bias in Machine Learning. 2020. *Scalable Path:* website. URL: www.scalablepath.com/machine-learning/bias-machine-learning

зареєстровані поліцейським управлінням Окленду злочини, пов'язані з наркотиками. Управління використовувало спеціальний алгоритм обробки великих даних для прогнозування наркозлочинів. Звичайно, HRDAG виявила, що прогностична модель майже виключно зосередилася на неєвропеоїдних спільнотах з низьким рівнем доходу. Але дані громадської охорони здоров'я щодо споживачів наркотиків у поєднанні з даними перепису населення США показали, що розподіл споживачів наркотиків не корелює з прогнозами програми, демонструючи, що прогнози алгоритму базувалися на упередженості, а не на реальності[1].

Показовим є те, що у червні 2020 р. міська рада Санта Круз, американського міста, яке одним з перших почало застосовувати для потреб поліції технології розпізнавання обличчя та прогнозування злочинів, відмовилася від використання таких систем ураховуючи численні прояви упередженості їх роботи та недостатню ефективність. Рішення полягало в забороні використовувати обидві технології, за винятком схвалення міською радою на основі «висновків про те, що технологія і дані, які використовуються для цієї технології, відповідають науково підтвердженим та рецензованим дослідженням, захищають і охороняють цивільне населення, права і свободи всіх людей і не увічнюють упередженість»[2].

Крім зазначених проблем з дискримінацією, багато питань виникає й через непрозорість функціонування зазначених систем. Як зазначалося раніше, покрокове відстеження рішень, що приймається подібними системами, є доволі складною проблемою. І якщо такі ризики є допустимим під час, наприклад, автоматизованого перекладу текстів з остаточним їх редагуванням людиною, то в ситуації, коли такі алгоритми використовуються в сфері юстиції, вони мають бути максимально відкритими та прозорими[3].

---

[1] Lum K., Isaac W. To predict and serve? *Significance.* 2016. № 13(5). Pp. 14–19. URL: http://dx.doi.org/10.1111/j.1740–9713.2016.00960.x

[2] Ibarra N. Santa Cruz becomes first U. S. city to approve ban on predictive policing. 2020. *Santa Cruz Sentinel*: website. URL: www.santacruzsentinel.com/2020/06/23/santa-cruz-becomes-first-u-s-city-to-approve-ban-on-predictive-policing/

[3] Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing. 2020. *Electronic Frontier Foundation*: website. URL: www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-only-weaponize-proximity-policing

Подібні небезпеки властиві не тільки сфері охорони правопорядку. Накопичений досвід та «критична» маса загроз неконтрольованого розширення сфери застосування систем ШІ зумовили появу законодавчих ініціатив, спрямованих на створення комплексної нормативно-правової бази для забезпечення відповідального розвитку ШІ, захисту основних прав і сприяння інноваціям. Як найбільш актуальні треба зазначити розпочаті урядом США 13.04.2023 р. громадські обговорення щодо «політики підзвітного штучного інтелекту»[1], а також обговорення проєкту, презентованого Європейською Комісією у квітні 2021 р., під назвою «The proposal for a regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (далі – Artificial Intelligence Act, AIA) and Amending Certain Union Legislative Acts»[2].

AIA використовує поняття «система штучного інтелекту» та визначає його наступним чином: *програмне забезпечення*, яке:

а) розроблене з використанням одного або кількох підходів, що відносяться до:

- методів машинного навчання, включаючи контрольоване, неконтрольоване та навчання з підкріпленням, з використанням різноманітних методів, у тому числі глибокого навчання;
- методів, що ґрунтуються на логіці та знаннях, включаючи представлення знань, індуктивне (логічне) програмування, бази знань, логічні та дедуктивні механізми, (символічні) міркування та експертні системи;
- статистичних методів, включаючи байєсовську оцінку, методи пошуку та оптимізації;

б) може, для заданого набору визначених людиною цілей, генерувати результати, такі як контент, прогнози, рекомендації, або рішення, що впливають на середовище, з яким вони взаємодіють.

---

[1] Accountability Policy Request for Comment. 2023. *Federal Register*: website. URL: www.federalregister.gov/documents/2023/04/13/2023–07776/ai-accountability-policy-request-for-comment

[2] Proposal For a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, 2021/0106(COD), 2021. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Визначення з усією очевидністю свідчить про фокус європейських законодавців на суто практичних питаннях використання продуктів, що вже існують або можуть бути створені.

У AIA програми ШІ класифікуються на основі потенційних рівнів ризику. Категорія «неприйнятний ризик штучного інтелекту» забороняє розробку та використання певних програм ШІ, наприклад систем соціального скорингу. До «штучного інтелекту високого ризику» віднесено системи, що можуть поставити під загрозу безпеку людей або порушити їхні основні права.

Авторами AIA реалізовано ідею нормативної мінімізації вказаних раніше соціальних ризиків впровадження ШІ. Порушення приватності пропонується контролювати у спосіб класифікованих за рівнем ризику вимог щодо розробки, введення в експлуатацію та використання систем ШІ.

Небезпеки впливу на поведінку людини, мінімізуються шляхом заборони окремих видів ШІ, які пропонується відносити до «Prohibited Artificial Intelligence Practices» (Article 5, AIA). Такі системи характеризуються «неприйнятним ризиком» та поділяються на 4 категорії: дві з них стосуються когнітивного поведінкового маніпулювання людьми або певними вразливими групами; інші 2 заборонені категорії – це системи соціального скорингу та системи біометричної ідентифікації в режимі реального часу та на відстані. Однак для кожної категорії є винятки з основного правила[1].

Непрозорість пропонується долати шляхом обов'язкового документування створення, використання та вдосконалення високоризикованих систем ШІ, постійної актуалізації технічної документації таких систем, наявністю обов'язку виробника надавати контролюючим органам вичерпну інформацію стосовно поточного стану системи ШІ, що віднесено до високоризикованих.

Нарешті, мінімізація упередженості забезпечується шляхом контролю за змістом та репрезентативністю навчальних, валідаційних та тестових наборів даних.

---

[1] Kop M. EU Artificial Intelligence Act: The European Approach to AI. *Transatlantic Antitrust and IPR Developments*. 2021. №2. Pp. 8–18. URL: https://law.stanford.edu/publications/euartificial-intelligence-act-the-european-approach-to-ai/

Важливими є положення AIA щодо підтримки досліджень та інновації в області ШІ. Зокрема, пропонується механізм «регуляторних пісочниць» (regulatory sandboxes), регуляторних інструментів, що дозволяють підприємствам тестувати та експериментувати з новими та інноваційними продуктами чи послугами під наглядом регулятора протягом обмеженого періоду часу. Регуляторні пісочниці виконують подвійну роль: 1) сприяють бізнес-навчанню, тобто розробці та тестуванню інновацій у реальному середовищі; та 2) забезпечують підтримку регуляторного навчання, тобто формулювання експериментальних правових режимів для керівництва та підтримки бізнесу в їх інноваційній діяльності під наглядом регуляторного органу. На практиці підхід спрямований на те, щоб уможливити експериментальні інновації у межах контрольованих ризиків і нагляду, а також покращити розуміння регуляторами нових технологій[1].

Значну увагу AIA приділяє системам ШІ, що використовують правоохоронні органи. Певні інструменти ШІ в правоохоронних органах віднесено до категорії «високого ризику» (AIA Annex III). Йдеться про системи призначені для:

- віддаленої біометричної ідентифікації;
- індивідуальної оцінки ризику вчинення правопорушення або ризику потенційних жертв кримінальних правопорушень;
- використання правоохоронними органами як поліграфи та подібні інструменти або для виявлення емоційного стану фізичної особи;
- виявлення діпфейків;
- оцінки достовірності доказів під час розслідування кримінальних правопорушень;
- прогнозування вчинення кримінального правопорушення на основі профілювання фізичних осіб, оцінки рис особистості, минулої злочинної поведінки фізичних осіб або груп;

[1] Madiega T., Van De Pol A. Artificial intelligence act and regulatory sandboxes. 2022. P. 6. *European Parliamentary Research Service*: website. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf

– профілювання фізичних осіб під час виявлення, розслідування або судового розгляду кримінальних правопорушень;

– кримінального аналізу, що дозволяє правоохоронним органам здійснювати пошук у складних пов'язаних і непов'язаних великих наборах даних, доступних у різних джерелах даних або в різних форматах даних, з метою виявлення невідомих закономірностей або виявлення прихованих зв'язків у даних[1].

Оскільки такі системи віднесено до високоризикових, їх користувачі, постачальники, розробники та продавці повинні дотримуватися передбачених AIA вимог. Зокрема, кожна програма повинна пройти вичерпний процес оцінки та зменшення ризиків (оцінка відповідності). Висуваються вимоги до даних, які використовуються для навчання цих систем ШІ, їх набори мають бути достатніми, щоб попередити дискримінаційні результати та алгоритмічні упередження[2]. Сертифікація, оцінка та моніторинг високоризикованих систем ШІ має відбуватися спеціальним уповноваженим органом, такі системи мають бути зареєстрованими та включеними у відповідну базу даних, має бути забезпечений постійний процес запису та зберігання відомостей щодо всіх подій, які відбуваються у системі, необхідним є забезпечення надійності функціонування та кіберзахисту системи тощо.

Ключовою вимогою до постачальників високоризикованих ШІ є вимога створення комплексної системи управління якістю (Art. 17 AIA), що має включати:

– стратегію дотримання вимог AIA, включаючи виконання процедур оцінки відповідності та внесення змін до системи;

– техніки контролю якості та забезпечення якості;

– процедури випробування, тестування та підтвердження, які мають бути виконані перед, під час і після розробки системи;

– технічні специфікації, включаючи стандарти, які мають бути застосовані;

[1] Proposal For a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, 2021/0106(COD), 2021. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[2] The EU AI act. *AP4AI*: website. URL: https://ap4ai.eu/eu-ai-act

– системи та процедури управління даними, включаючи збір даних, аналіз, маркування даних, зберігання даних, фільтрацію даних, добування даних, агрегацію даних, збереження даних та будь-яку іншу операцію, пов'язану з даними, яка виконується для введення в експлуатацію високоризикових систем ШІ;

– систему управління ризиками, як безперервний ітераційний процес, який виконується протягом усього життєвого циклу системи, що систематично оновлюється;

– системи моніторингу після введення в експлуатацію;

– процедури, повідомлення про серйозні інциденти;

– процедури взаємодії з національними уповноваженими органами;

– системи та процедури зберігання всієї відповідної документації та інформації;

– управління ресурсами, включаючи заходи забезпечення безпеки постачання;

– кадрову політику, включаючи визначення відповідальності керівництва за напрямами системи забезпечення якості[1].

Настільки багато уваги деталям ми приділили, оскільки вважаємо, що вони найкраще демонструють, як змінилася дискусія стосовно правового регулювання соціалізації ШІ. Цілком природньо, що починалася вона з питань стратегічного рівня, але фактичні інформаційні технології, їх використання та розширення сфери застосування достатньо чітко визначили напрями подальшого розвитку дискурсу. Фокус змістився на чіткі прикладні задачі, дискусія набула традиційного юридичного характеру та змісту.

Законопроєкт отримав переважно схвальні відгуки науковців, водночас були представлені й критичні позиції. Наприклад, на думку М. Веле та Ф. Зуйдервена Боргесіуса, AIA «зібраний із законодавства про безпеку продукції 1980-х років, захисту основних прав, нагляду та захисту споживачів», такий підхід не дозволяє розглядати законопроєкт як всеосяжний та позбавлений істотних пробілів. Наприклад,

[1] Accountability Policy Request for Comment. 2023. *Federal Register*: website. URL: <www.federalregister.gov/documents/2023/04/13/2023–07776/ai-accountability-policy-request-for-comment

положення про прозорість або мало додають до чинного законодавства, або викликають більше запитань, ніж відповідей, коли розглядаються їхні наслідки[1].

Новий виток дискусії з'явився з появою ChatGPT. Виникло питання, чи може генеративний ШІ загального призначення бути використаним для заподіяння шкоди, чи може він стати частиною злочинного використання ШІ та, відповідно, чи не підлягатиме він забороні як один з видів «Prohibited Artificial Intelligence Practices». Гіпотетично, представлені у відкритому доступі системи ШІ, такі як ChatGPT, Midjourney або DALL E, можуть, та, скоріше за все, будуть використовуватися для вчинення злочинів. Чи означає це, що вони мають бути забороненими? Зрозуміло ні. Європейські законодавці без сумніву знайдуть збалансоване рішення. Дискусія триває[2].

1.3. Міжнародна регламентація питань формування інформаційного простору

Як уявляється, досягнення належного рівня інформаційної безпеки є можливим і завдяки формуванню безпечного та надійного інформаційного простору, ключовими аспектами якого виступають: сприяння довірі та впевненості; захист приватності та персональних даних; стійкість до кіберзагроз; збереження демократичних цінностей; заохочення інновацій та співпраці; розвиток позитивної цифрової культури; сприяння цифровій інклюзії; підтримка економічного зростання; сприяння міжнародному співробітництву тощо. З цього ви-

[1] Veale M., Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International.* 2021. № 21(4). Pp. 97–112. URL: http://dx.doi.org/10.9785/cri-2021-220402

[2] Hacker P., Engel A., Mauer M. Regulating ChatGPT and other Large Generative AI Models. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. Association for Computing Machinery (June 2023). 2023. Pp. 1112–1123. URL: https://doi.org/10.1145/3593013.3594067

пливає, що різноманітні шкідливі елементи інформаційного простору мають значний негативний вплив на його формування та «здоров'я».

На цьому етапі дослідження обмежимось питанням аналізу міжнародних ініціатив з приводу таких деструктивних проявів інформаційного простору, як пропаганда війни, дезінформація та мова ворожнечі з огляду на їх логічну пов'язаність та, подекуди, взаємообумовленість.

При цьому акцентуємо увагу, що означені питання знаходяться у тісному взаємозв'язку з правом особи на свободу слова та вираження поглядів (ст. 19 Загальної декларації прав людини від 10.12.1948 р. (далі – Декларація), ст. 19 Міжнародного пакту про громадянські і політичні права від 16.12.1966 р. (далі – Пакт, МПГП)), ст. 10 Конвенції Ради Європи про захист прав людини і основоположних свобод від 04.11.1950 р. (далі – ЄКПЛ)). Адже, як пропаганда війни, так і дезінформація та мова ворожнечі є по суті інформаційними актами, формою комунікації або поширення інформації.

Тому, з одного боку, як писав колись давньогрецький поет-драматург Еврипід, не говорити своїх думок – це рабство. І, як зазначається у звіті Спеціального доповідача ООН з питань заохочення та захисту права на свободу думки та її вільне вираження, в ООН вже давно просувається ідея про те, що свобода вираження поглядів має фундаментальне значення для участі громадськості та дебатів, підзвітності, сталого розвитку та людського розвитку, а також для здійснення всіх інших прав, а самовираження може викликати суперечки, дискусії, навіть гнів або смуток – але аж ніяк не покарання, страх і мовчання[1].

Проте з іншого боку, реальна та практична реалізація ідеї «абсолютної свободи слова», якою б привабливою вона не була, не видається досяжною з огляду на ті ризики, які потенційно вона може містити. Одним із таких зворотних боків необмеженості свободи

[1] Promotion and protection of the right to freedom of opinion and expression: Note by the Secretary-General. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on 6 September 2016 № A/71/150. P. 3. *General Assembly of the United Nations*: of. website. URL: https://freedex.org/wp-content/blogs.dir/2015/files/2017/05/FOE-worldwide-report.pdf

слова і є практика пропаганди війни, дезінформації та мови ворожнечі. У зв'язку з цим аналіз їх міжнародно-правової регламентації вважаємо за необхідне додатково здійснювати крізь призму статей, що регламентують свободу слова та вираження поглядів.

Пропаганда війни. Пропаганда війни завдає шкоду (або загрозу її спричинення) інформаційному простору за рахунок спотворення фактів, маніпулювання громадською думкою та сприяння поширенню дезінформації. Вона може створити вороже і роз'єднуюче інформаційне середовище, загострити міжнародні відносини, посилюючи недовіру і ворожість між державами, стати передвісником деяких з найсерйозніших порушень міжнародного права, як-от, підбурювання до геноциду, воєнні злочини і злочини проти людяності, а також стати інструментом для виправдання або применшення їх наслідків.

Саме тому її заборона в міжнародному праві переплітається з еволюцією норм, загалом спрямованих на запобігання війні. Так, у цьому контексті першочергово варто звернути увагу на приписи Гаазьких конвенцій 1899 р. та 1907 р., що хоча прямо і не стосуються пропаганди війни, але містять вихідні положення, які покликані регулювати поведінку держав під час збройних конфліктів.

Що характерно, до 1930-х років проблема деструктивної пропаганди як така найчастіше розглядалася на рівні двосторонніх угод держав про дружбу та ненапад, а першою багатосторонньою угодою, безпосередньо спрямованою на окреслення цієї проблематики, стала Міжнародна конвенція про використання телерадіомовлення в інтересах миру[1], ухвалена Лігою Націй 23.09.1936 р.[2] Цим міжнародним актом безпосередньо встановлювалась заборона та накладався обов'язок припиняти будь-які трансляції в межах територій держав-

[1] International Convention concerning the Use of Broadcasting in the Cause of Peace. Signed at Geneva, September 23rd, 1936. *Worldlii*: website. URL: http://www.worldlii.org/int/other/treaties/LNTSer/1938/80.html

[2] Після Другої світової війни функції депозитарію Конвенції перейшли від Ліги Націй до ООН, Генеральна Асамблея якої у своїй резолюції № 841 (IX) від 17.12.1954 р. визнала її положення важливим елементом у сфері свободи інформації (Див.: International Convention concerning the Use of Broadcasting in the Cause of Peace (Geneva, 1936). *United Nations Dag Hammarskjöld Library*: of. website. URL: https://digitallibrary.un.org/record/211972?ln=ru).

підписантів, які носять такий характер, що підбурює населення будь-якої території до дій, несумісних із внутрішнім порядком або безпекою території або таких, що підбурюють до війни проти іншої високої договірної сторони[1].

Однак тут варто зауважити, що такі країни як Німеччина, Італія та Японія, що розгорнули широку пропагандистську діяльність протягом 1930-х – 1940-х років, не були сторонами Конвенції, що значно обмежило сферу її дії та, фактично, не виправдало мету її ухвалення на передодні Другої світової війни. Саме в цей час зросло усвідомлення необхідності всеосяжних правил для захисту тих, хто постраждав від збройних конфліктів, результатом чого стало розроблення та прийняття Статуту ООН від 26.06.1945 р. (ст. 39 якого може бути практично застосованою до пропаганди війни)[2], Статуту Нюрнберзького трибуналу від 08.08.1945 р. та Женевських конвенцій 1949 р.

Так, зокрема, Статут Нюрнберзького трибуналу, визначаючи індивідуальну кримінальну відповідальність за злочини проти миру, людяності та воєнні правопорушення, зазначав, що керівники, організатори, *підбурювачі* та пособники, які брали участь у складанні або

---

[1] Окремо варто наголосити, що рф як держава-правонаступник СРСР є учасницею цієї Конвенції, і по суті випадки російської дезінформації, військової пропаганди та інших інформаційних операцій, які «шкодять доброму міжнародному взаєморозумінню» між державами-учасницями, підпадають під дію її норм-заборон. І оскільки Конвенція містить зобов'язання erga omnes, всі держави-учасниці (серед яких, зокрема, і деякі члени НАТО, такі як Норвегія, Фінляндія, Естонія, Данія, Люксембург, Латвія, Угорщина та Болгарія) мають право посилатися на порушення рф статей цього міжнародного акту щодо інформаційних операцій, які призвели до вторгнення в Україну і виправдовують його (див.: Talita de Souza Dias. Russia's «genocide disinformation» and war propaganda are breaches of the International Convention Concerning the Use of Broadcasting in the Cause of Peace and fall within the ICJ's jurisdiction. 2022. *Blog of the European Journal of International Law*: website. URL: https://www.ejiltalk.org/russias-genocide-disinformation-and-war-propaganda-are-breaches-of-the-international-convention-concerning-the-use-of-broadcasting-in-the-cause-of-peace-and-fall-within-the/)

[2] Рада Безпеки визначає існування будь-якої загрози миру, будь-якого порушення миру або акту агресії та надає рекомендації або вирішує те, які дії варто почати у відповідності зі статтями 41 та 42 для підтримки або відновлення міжнародного миру й безпеки (Див.: Організація Об'єднаних Націй. Статут Організації Об'єднаних Націй від 26 червня 1945 року. С. 28. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf)

у здійсненні спільного плану або змови, спрямованої на вчинення будь-яких із вищезазначених злочинів, несуть відповідальність за всі дії, вчинені будь-якими особами з метою здійснення такого плану[1]. Це, зі свого боку, стало правовою базою для притягнення до відповідальності головних пропагандистів третього рейху Юліуса Штрайхера (головного редактора нацистського тижневика «Der Stürmer») та Отто Дітріха (шефа преси НСДАП), які «заразили свідомість німців вірусом антисемітизму та підбурили німецький народ до активного переслідування»[2].

Дещо пізніше у *резолюції № 110 (II) від 03.11.1947 р.* Генеральна Асамблея безпосередньо засудила всі форми пропаганди, в якій би країні вона не велася, що має на меті або може спровокувати чи заохотити будь-яку загрозу миру, порушення миру або акт агресії та заохотила уряди держав вжити відповідні заходи з метою сприяння дружнім відносинам між народами, а також спонукання розповсюдження інформації, покликаної виразити безсумнівне прагнення всіх народів до миру.[3]

Наступним логічним кроком у регламентації пропаганди на міжнародному рівні стало розроблення МПГП, у ст. 20 якого була висловлена однозначна позиція щодо повної заборони на будь-яку пропаганду війни [4]. Тут також варто підкреслити, що, як зазначалось на початку підрозділу, за своєю суттю пропаганда війни є проблемою у межах свободи слова і представляє собою зловживанням цим пра-

---

[1] Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal. London, 8 August 1945. *International Humanitarian Law Databases*: of. website. URL: https://ihl-databases.icrc.org/en/ihl-treaties/nuremberg-tribunal-charter-1945/article-6b

[2] Gordon, Gregory S., The Propaganda Prosecutions at Nuremberg: The Origin of Atrocity Speech Law and the Touchstone for Normative Evolution (January 16, 2017). *Loyola of Los Angeles International and Comparative Law Review*. 2017. Vol. 39, №1. Pp. 209–245. URL: https://ssrn.com/abstract=2958011 235

[3] UN General Assembly. *Measures to be taken against propaganda and the inciters of a new war*, 3 November 1947, A/RES/110. *Refworld*: of. website. URL: https://www.refworld.org/docid/3b00f08e58.html

[4] Міжнародний пакт про громадянські і політичні права: Міжнародний документ від 16.12.1966. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

вом. Так, у коментарі до ст. 19 МПГП Комітет з прав людини підкреслює, що ст.ст. 19 і 20 є сумісними та доповнюють одна одну. Дії, про які йдеться у ст. 20, підлягають обмеженню відповідно до трискладового тесту, викладеного у ч. 3 ст. 19 (передбаченення обмеження в законі, переслідування легітимної мети та необхідність у суспільстві). Те, що відрізняє дії, передбачені ст. 20, від інших дій, які можуть підлягати обмеженню відповідно до п. 3 ст. 19, полягає в тому, що для перших, Пакт вказує на конкретну реакцію, яка вимагається від держави: заборона в законі. Лише в цьому сенсі ст. 20 може розглядатися як lex specialis відносно ст. 19[1].

При цьому з огляду на невизначеність на рівні Пакту поняття «пропаганда» виникло питання, чи обмежується вона лише «підбурюванням до війни», або поширюється на «пропаганду, яка передує прямому підбурюванню до війни, але слугує або засобом підготовки до майбутньої війни, або, можливо, перешкоджає мирному врегулюванню спорів»[2].

У коментарі з цього приводу зауважується, що така заборона згідно з пунктом 1 поширюється на всі форми пропаганди, що *загрожує або призводить до акту агресії чи порушення миру*, що суперечить Статуту ООН, тоді як пункт 2 спрямований проти будь-якої пропаганди національної, расової чи релігійної ненависті, яка становить підбурювання до дискримінації, ворожнечі чи насильства, незалежно від того, чи має така пропаганда чи захист інтересів внутрішні чи зовнішні цілі відповідної держави.[3]

---

[1] Human Rights Committee. General comment № 34. Article 19: Freedoms of opinion and expression on 12 September 2011. 13 p. *United Nations*: of. website. URL: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

[2] Centre for Law and Democracy. Submission to the UN Special Rapporteur on Freedom of Expression on Challenges to Freedom of Expression in Times of Armed Conflict. July 2022. *Centre for Law and Democracy*: of. website. URL: https://www.law-democracy.org/live/wp-content/uploads/2022/07/UN-SR.Submission-on-FOE-and-Armed-Conflict.Jul22.pdf

[3] Office of the United Nations High Commissioner for Human Rights. General Comment № 11: Prohibition of propaganda for war and inciting national, racial or religious hatred (Art. 20). 29/07/1983. CCPR General Comment № 11. (General Comments). URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf

Тобто для того, щоб пропаганда справді становила загрозу війни або призвела до війни, вона має ймовірно спровокувати війну найближчим часом[1].

Іншим дискусійним питанням у цьому аспекті є розуміння поняття «війна» і, відповідно, чи охоплює воно неміжнародні конфлікти. Деякі вчені зауважують, що так звані «громадянські війни» не підпадають під дію ст. 20 Пакту «поки вони не переростають у міжнародний конфлікт».[2] З чим погоджуються і експерти ООН, зазначаючи, що «війна» означає акт агресії, який суперечить Статуту ООН і не охоплює громадянські війни, внутрішні чвари, війни, спрямовані на самовизначення чи незалежність, або використання застосування сили при самообороні[3].

Ще одним питання, пов'язаним із застосуванням цієї норми, є визначення часових меж дії такої пропаганди, тобто охоплює вона період перед війною чи після. З цього приводу влучно висловився ЄСПЛ (зокрема, у справі щодо накладення санкцій на Sputnik), зазначивши, що ця заборона «включає не тільки підбурювання до майбутньої війни, але також безперервні, повторювані та узгоджені заяви на підтримку триваючої війни, що суперечить міжнародному праву, зокрема, якщо заяви походять від медіа, які прямо чи опосередковано контролюються державою-агресором»[4].

Також варто зазначити, що така заборона має бути імперативною і, більше того, навіть оголошення надзвичайного стану не може слугувати виправданням для її застосування[5].

---

[1] Aswad Evelyn. Propaganda for War & International Human Rights Standards (March 1, 2023). *Chicago Journal of International Law*. 2023. Vol. 24, №1. URL: https://ssrn.com/abstract=4544429

[2] Michael Kearney. The Prohibition of Propaganda for War in the International Covenant on Civil and Political Rights. *Netherlands Quarterly of Human Rights*, 2005. №*23*(4). P. 562. URL: https://doi.org/10.1177/016934410502300402

[3] Aswad Evelyn. Propaganda for War & International Human Rights Standards (March 1, 2023). *Chicago Journal of International Law*. 2023. Vol. 24, №1. URL: https://ssrn.com/abstract=4544429

[4] Тетяна Авдєєва, Максим Дворовий. По кому подзвін: Відповідальність за дезінформацію під час війни: аналітичний звіт. Лабораторія цифрової безпеки, Київ, 2022. С. 21. URL: https://dslua.org/wp-content/uploads/2023/02/Analitychne-doslidzhennia.-Vidpovidalnist-za-dezinformatsiiu-pid-chas-viyny.pdf

[5] General comment №29. States of emergency (article 4) International Covenant on Civil and Political Rights on 31 August 2001. 8 p. *United Nations*: of. website. URL: https://digitallibrary.un.org/record/451555

Наступним актом у досліджуваній сфері є Заключний акт Наради з питань безпеки та співробітництва в Європі від 01.08.1975 р., одним із принципів якого було задекларовано сприяння всіма засобами, що кожна із сторін визнає придатними, створенню атмосфери довіри та поваги між народами, що відповідає їхньому обов'язку утримуватися від пропаганди агресивних війн або будь-якого застосування сили чи погрози силою, несумісного з цілями ООН і з Декларацією принципів, якими держави-учасниці зобов'язалися керуватися у взаємних відносинах [1].

Щодо основоположних європейських положень у сфері захисту прав і свобод людини – ЄКПЛ та Хартії Європейського Союзу про основні права (далі – Хартія ЄС), – то безпосередні заборони на пропаганду війни в них не містяться, хоча практично застосованими у цьому випадку є положення, що регламентують питання зловживання правами (ст. 17 та ст. 54 відповідно).

Дезінформація. Питанням, логічно пов'язаним із забороною пропаганди війни, є регулювання дезінформації у міжнародно-правовому вимірі, яка так само здійснює руйнівний і далекосяжний вплив на інформаційний простір на рівні як окремих людей, суспільства, так і навіть геополітичних ландшафтів. Дезінформація сприяє поширенню неправдивих наративів, шкідливих стереотипів, дискримінації та мови ворожнечі (про що буде йти мова нижче), нарощуванню соціальної поляризації, а також може використовуватися як інструмент у гібридній війні та геополітичних конфліктах.

Практично застосованими для врегулювання дезінформації на міжнародному рівні є положення вище згаданої *Міжнародної конвенції про використання телерадіомовлення в інтересах миру від 23.09.1936 р.*, у ст. 3 якої зазначається, що сторони зобов'язуються взаємно забороняти і, у відповідних випадках, негайно припиняти на своїх територіях будь-які дії, здатні завдати шкоди міжнародному взаєморозумінню через твердження, про неправдивість яких особи, відповідальні за розповсюдження, знають або повинні знати. Також

[1] Organization for Security and Co-operation in Europe. Helsinki Final Act on 1 August 1975. *Organization for Security and Co-operation in Europe*: of. website. URL: https://www.osce.org/helsinki-final-act

вони взаємно зобов'язуються забезпечити, щоб будь-яка помилка, яка може зашкодити доброму міжнародному взаєморозумінню через неточні твердження, була якомога швидше виправлена найефективнішими засобами, навіть якщо неточність стає очевидною лише після її розповсюдження[1].

Окрім цього, з метою висвітлення досліджуваного питання свого часу було прийнято *Резолюцію Генеральної Асамблеї ООН від 15.11.1947 р. № 127(III)*, у якій підкреслювалося, що покращення взаєморозуміння та дружніх відносин між державами може бути досягнуто за рахунок вжиття заходів для боротьби з розповсюдженням неправдивих та перекручених повідомлень.[2]

Тут також варто згадати і *Декларацію про основоположні принципи, що стосуються внеску засобів масової інформації у зміцнення миру і міжнародного взаєморозуміння, у заохочення прав людини і в боротьбу з расизмом, апартеїдом і підбурюванням до війни від 28.11.1978 р.,* якою виголошується роль ЗМІ у зміцненні миру, міжнародного взаєморозуміння, а також просування прав людини[3].

Треба підкреслити, що питання дезінформації також безпосередньо пов'язані із застосуванням ст. 19 МПГП[4]. При цьому відповідні органи ООН з прав людини неодноразово заявляли, що криміналізація дезінформації є несумісною з правом на свободу вираження поглядів. Так, коментуючи національну правову систему Камеруну, Комітет ООН з прав людини заявив, що переслідування і покарання

[1] Convention internationale concernant 1'emploi de]a radiodiffusion dans I'intiret de]a paix. Signee i Geneve, le 23 septembre 1936. *Societe'des Nations – Recuei des Traites*. № 4319. 1938. Pp. 302–317. URL: https://docs.pca-cpa.org/2016/01/International-Convention-concerning-the-Use-of-Broadcasting-in-the-Cause-of-Peace-1936.pdf

[2] False or distorted reports: Resolution adopted by the General Assembly during its 2nd session, 16 September-29 November 1947. A/519. 1948. Pp. 38–39. *United Nations Dag Hammarskjöld Library*: of. website. URL: https://digitallibrary.un.org/record/209899?ln=ru

[3] Declaration on Fundamental Principles concerning the Contribution of the Mass Media to Strengthening Peace and International Understanding, to the Promotion of Human Rights and to Countering Racialism, Apartheid and Incitement to War on 28 November 1978. *UNESCO*: of. website. URL: https://en.unesco.org/about-us/legal-affairs/declaration-fundamental-principles-concerning-contribution-mass-media

[4] Міжнародний пакт про громадянські і політичні права: Міжнародний документ від 16.12.1966. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

журналістів за злочин публікації неправдивих новин лише на тій підставі, що ці новини були неправдивими, є явним порушенням ст.19 МПГП.[1]

На додаток до цього, як зазначається *в Спільній декларації щодо свободи вираження поглядів і «фейкових новин», дезінформації та пропаганди від 03.03.2017 р.*, загальні заборони на поширення інформації, заснованої на нечітких і двозначних ідеях, включаючи «неправдиві новини» або «необ'єктивну інформацію», є несумісними з міжнародними стандартами щодо обмежень свободи вираження поглядів і мають бути скасовані. Так само зауважується, що кримінальне законодавство про наклеп є надмірно обмежувальним і має бути скасоване. Норми цивільного права про відповідальність за неправдиві та наклепницькі заяви є законними лише тоді, коли відповідачам надаються повну можливість довести правдивість цих тверджень, а також скористатися іншими засобами захисту, наприклад, справедливими коментарями.[2]

Більш розгалуженим у досліджуваній царині є європейське законодавство. Так, у *Рекомендації CM/Rec(2018)2 Комітету Міністрів державам-членам щодо ролі та обов'язків інтернет-посередників від 07.03.2018 р.* підкреслюється, що цілеспрямовані дезінформаційні кампанії в інтернеті, розроблені спеціально для того, щоб посіяти недовіру і плутанину та загострити існуючі розбіжності в суспільстві, можуть мати дестабілізуючий вплив на демократичні процеси[3].

Окрім цього, *Резолюція Європейського парламенту від 23.11.2016 р. щодо стратегічної комунікації ЄС для протидії пропаганді третіх сторін* визначає дезінформацію як складову частину гібридної війни,

---

[1] International law and policy on disinformation in the context of freedom of the media: Brief Paper for the Expert Meeting organized by the Office of the OSCE Representative on Freedom of the Media on 14 May 2021 / Prepared by Dr. Andrey Rikhter. Vienna, May 2021. 27 p. URL: https://www.osce.org/files/f/documents/8/a/485606.pdf

[2] Joint Declaration on freedom of expression and «fake news», disinformation and PROPAGANDA № FOM.GAL/3/17 on 3 March 2017. URL: https://www.osce.org/files/f/documents/6/8/302796.pdf

[3] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies). *Council of Europe*: of. website. URL: https://rm.coe.int/0900001680790e14

а також робить акцент на аспектах інформаційного впливу зі сторони рф та ІДІЛу[1]. У *Резолюції про іноземне втручання в усі демократичні процеси в Європейському Союзі, включаючи дезінформацію, від 09.03.2022 р.* у продовження цих положень Європейський парламент називає дезінформацію однією із форм іноземного втручання та закликає Комісію запропонувати, а співзаконодавців та держав-членів підтримати багаторівневу, скоординовану та міжгалузеву стратегію, а також адекватні фінансові ресурси, спрямовані на забезпечення ЄС та його держав-членів відповідною політикою передбачення та стійкості, а також інструментами стримування, що дозволить їм протистояти всім гібридним загрозам та атакам, організованим іноземними державними та недержавними суб'єктами[2]

Достатньо плідною є діяльність і Європейської комісії, що ухвалила низку ініціатив з питань боротьби з дезінформацією, серед яких:

1. Спільна рамкова програма протидії гібридним загрозам –відповідь Європейського Союзу від 06.04.2016 р., у якій зазначається, що держави-члени повинні розробити скоординовані механізми стратегічної комунікації для забезпечення достовірності інформації та протидії дезінформації з метою викриття гібридних загроз (зокрема, інструменти соціальних медіа, використання фахової допомоги лінгвістів і спеціалістів із соціальних мереж)[3].

2. Повідомлення «Боротьба з дезінформацією в Інтернеті: європейський підхід» від 26.04.2018 р., де надано визначення дезінформації (як достовірно неправдивої або оманливої інформації, що створюється, подається та поширюється з метою отримання економічної

---

[1] European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)). *European Parliament*: of. website. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html?redirect

[2] European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)). *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022IP0064&qid=1701100508683

[3] Joint Framework on countering hybrid threats a European Union response: Joint Communication to the European Parliament and the Council № JOIN(2016) 18 final on 6.4.2016. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

вигоди або навмисного введення громадськості в оману, а також може завдати шкоди суспільству), аналізуються її причини, а також викладаються головні принципи та цілі, якими мають керуватися держави у процесі боротьби з нею[1].

Так, означеними принципами є прозорість інформації, сприяння її різноманітності, підвищення довіри до інформації та впровадження інклюзивних рішень, а цілями, відповідно, 1) більш прозора, надійна та підзвітна онлайн-екосистема; 2) безпечні та стійкі виборчі процеси; 3) сприяння освіті та медіаграмотності; 4) підтримка якісної журналістики як важливого елементу демократичного суспільства; 5) протидія внутрішнім і зовнішнім дезінформаційним загрозам через стратегічну комунікацію.

3. План дій щодо дезінформації від 05.12.2018 р., спрямований на посилення спроможності ЄС у боротьбі з дезінформацією та міждержавній співпраці, що ґрунтується на, так званих, чотирьох стовпах: 1) покращення спроможності інституцій Союзу виявляти, аналізувати та викривати дезінформацію; 2) посилення скоординованої та спільної відповіді на дезінформацію; 3) мобілізація приватного сектору для боротьби з дезінформацією; 4) підвищення обізнаності та покращення стійкості суспільства[2].

4. Кодекс практики боротьби з дезінформацією від 2018 р., розроблений на досягнення цілей, викладених у вищеозначеному повідомленні Європейської комісії, який представляє собою перелік стандартів саморегулювання для онлайн-платформ[3], представників ре-

---

[1] Tackling online disinformation: a European Approach: Communication from The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions № COM/2018/236 final on 26.4.2018. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

[2] Action Plan against Disinformation. Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions № JOIN(2018) 36 final on 5.12.2018. *EUR-lex*: of website. URL: https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

[3] До переліку онлайн-платформ, що добровільно долучилися до виконання приписів Кодексу, належать, зокрема, такі інформаційні «гіганти» як Facebook, Google, Twitter (X) і Mozilla.

кламної індустрії та підписантів щодо боротьби з поширенням дезінформації. Варто підкреслити, що в цьому акті було окремо зазначено, що поняття «дезінформація» *не включає* оманливу рекламу, помилки в репортажах, сатиру та пародію, а також чітко ідентифіковані партійні новини та коментарі, і не зачіпає обов'язкових юридичних зобов'язань, саморегульованих рекламних кодексів та стандартів щодо оманливої реклами[1].

5. Посилений кодекс боротьби з дезінформацією від 16.06.2022 р., відповідно до положень якого підписанти зобов'язалися вживати заходи у кількох сферах, таких як демонетизація поширення дезінформації, забезпечення прозорості політичної реклами, розширення прав і можливостей користувачів, посилення співпраці з фактчекерами та надання дослідникам кращого доступу до даних (загалом 44 зобов'язання та 128 конкретних заходів)[2] тощо.

У контексті останніх ініціатив також варто зазначити, що провідна роль у регулюванні інформаційного простору та моніторингу шкідливого контенту відводиться також *Директиві про аудіовізуальні медіа-послуги від 10.03.2010 р.*[3] та *Закону про цифрові послуги від 19.10.2022 р.*[4]

Мова ворожнечі. Третім деструктивним проявом інформаційного простору, що логічно доповнює пропаганду війни та дезінформацію, є мова ворожнечі, що представляє собою комунікацію в будь-якій формі, яка своїм змістом містить образу, погрозу конкретній особі

---

[1] 2018 Code of Practice on Disinformation. *European Commission*: of website. URL: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

[2] The 2022 Code of Practice on Disinformation. *European Commission*: of website. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[3] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010L0013&qid=1699218089896

[4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1701100248817

чи групі осіб залежно від її (їх) захищених ознак. Часто така практика спрямована на приниження та дегуманізацію окремих осіб або спільнот, що сприяє дискримінації, ворожнечі та, у крайніх випадках, насильству.

При цьому будучи за своєю суттю інформаційним актом мова ворожнечі так само, як щодо попередньо розглянутих елементів, потребує її комплексного розгляду разом із правом особи на свободу слова. Тут підкреслюємо, що у коментарі до Пакту акцентується увага, що, сферою дії ст. 19 охоплюються навіть висловлювання, що можуть вважатися глибоко образливими[1].

З приводу цього твердження, що показово, у Комітеті з прав людини свого часу розгадалось повідомлення, подане громадянином Канади Малькольмом Россом, з приводу оцінки висловлених ним поглядів щодо абортів, конфліктів між юдаїзмом і християнством та захисту християнської релігії. Національна Комісія з розслідування постановила, що в наявних висловлюваннях було багато посилань, які є prima facie дискримінаційними щодо осіб єврейської віри та походження; вони принижують віру та переконання євреїв і закликають християн не тільки поставити під сумнів обґрунтованість єврейських вірувань і вчень, але й зневажати віру та походження євреїв як такі, що підривають свободу, демократію, християнські переконання та цінності. Внаслідок цього заявник спочатку був відправлений у відпустку без збереження заробітної плати на тиждень, а потім переведений на невикладацьку роботу.

У цьому контексті Комітет постановив, що мало місце порушення ст. 19 Пакту з огляду на те, що усунення автора з посади вчителя можна вважати обмеженням, необхідним для захисту права і свободи єврейських дітей на шкільну систему, вільну від упереджень, забобонів і нетерпимості. Крім того, Комітет зазначив, що автора було призначено на непедагогічну посаду після мінімального періоду відпустки без збереження заробітної плати і що обмеження, таким чином,

[1] Human Rights Committee. General comment № 34. Article 19: Freedoms of opinion and expression on 12 September 2011. 13 p. *United Nations*: of. website. URL: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

не виходило за межі того, що було необхідним для виконання його захисних функцій[1].

Окрім цього, питання регламентації мови ворожнечі також пов'язані із утвердженням права особи на захист від дискримінації, відповіді приписи стосовно чого містяться у ст. 7 Декларації, ст. ст. 20, 26 МПГП, ст. 14 ЄКПЛ, Протоколі № 12 до ЄКПЛ, а також у *Міжнародній конвенції про ліквідацію всіх форм расової дискримінації від 21.12.1965 р.*[2].

Щодо останньої, то її положеннями, по-перше, оголошуються злочинами всяке поширення ідей, основаних на расовій перевазі або ненависті, всяке підбурювання до расової дискримінації, а також усі акти насильства або підбурювання до таких актів, спрямованих проти будь-якої раси чи групи осіб іншого кольору шкіри або етнічного походження, а також подання будь-якої допомоги для проведення расистської діяльності, включаючи її фінансування; оголошують протизаконними і забороняють організації, а також оголошуються протизаконними і забороняються організації, організовану і всяку іншу пропагандистську діяльність, які заохочують расову дискримінацію та підбурюють до неї, і визнається участь у таких організаціях чи в такій діяльності злочином, що карається законом (ст. 4). По-друге, держави-члени зобов'язуються вжити негайних і ефективних заходів, зокрема в галузях викладання, виховання, культури та інформації, в цілях боротьби із забобонами, які ведуть до расової дискримінації (ст. 7).

При цьому у Загальній рекомендації Комітету ООН з ліквідації расової дискримінації № 35 про боротьбу з використанням мови ворожнечі расистського характеру від 26.09.2013 р. уточняється, що стосовно таких дій, як поширення ідей і підбурювання до расової дискримінації треба враховувати такі чинники як: 1) зміст і форма висловлювання (як воно було сформульоване, у якій формі

[1] Ross v. Canada (Communication № 736/1997) on 26 October 2000. P. 16. *JURIS database*: of. website. URL: https://juris.ohchr.org/casedetails/902/en-US

[2] Міжнародна конвенція про ліквідацію всіх форм расової дискримінації: Міжнародний документ від 21.12.1965 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_105#Text

поширювалося, яким був стиль його вираження, чи не було воно провокативним та цілеспрямованим); 2) економічний, соціальний і політичний клімат на момент висловлювання і його поширення (чи була наявна системна дискримінація зокрема); 3) посада або становище того, хто виступає в суспільстві, та аудиторія, на яку розраховано висловлювання; 4) масштаби поширення висловлювання, включно з характером аудиторії та засобами його передачі (чи було воно поширено через ЗМІ або інтернет, в якому обсязі було здійснено, якими були масштаби повідомлення); 5) цілі висловлювання (якщо воно було спрямовано на захист або забезпечення прав окремих осіб або їх груп осіб, то воно не є кримінально караним)[1].

У цьому аспекті заслуговують на увагу також рекомендації для законодавців, що були наведені *у Рабатському плані дій щодо заборони пропаганди національної, расової або релігійної ненависті, що є підбурюванням до дискримінації, ворожнечі або насильства*, схваленому Радою з прав людини ООН у квітні 2013 року. Так, цим документом було запропоновано встановити високий поріг для визначення обмежень свободи вираження поглядів, підбурювання до ворожнечі та застосування ст. 19 МПГП. У зв'язку з цим було запропоновано шестиступеневий тест, що складається з критеріїв, які дають уявлення, що висловлювання має кримінально караний характер, що частково збігаються з тими, що були викладені у Загальній рекомендації Комітету ООН з ліквідації расової дискримінації № 35. Ними є: 1) соціальний і політичний контекст; 2) статус того, хто говорить; 3) намір викликати ворожість публіки до певної групи; 4) зміст і форма мови; 5) ступінь впливу промови та 6) ймовірність заподіяння шкоди, включно з її невідворотністю[2].

Окреме місце серед міжнародно-правових актів у цій царині займають *Стратегія та план дій ООН щодо боротьби з мовою ворож-*

[1] Committee on the Elimination of Racial Discrimination. General recommendation №. 35 Combating racist hate speech on 26 September 2013. *Refworld*: of. website. URL: https://www.refworld.org/docid/53f457db4.html

[2] Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred on 11 January 2013. 15 p. *United Nations*: of. website. URL: https://www.ohchr.org/sites/default/files/Rabat_draft_outcome.pdf

нечі, ухвалені 18.06.2019 р., де Генеральний секретар ООН Антоніу Гутерреш підкреслив, що подолання мови ворожнечі не означає обмеження чи заборону свободи слова. Це означає запобігти переростанню мови ворожнечі в щось більш небезпечне, зокрема підбурювання до дискримінації, ворожнечі та насильства, що заборонено міжнародним правом[1].

Головними цілями цих документів проголошено: посилення зусиль ООН, спрямованих на скоординоване усунення першопричин і рушійних факторів мови ворожнечі; зосередження уваги на реакції ООН на вплив мови ворожнечі на суспільство.

Так само Стратегія ґрунтується на таких принципах як: 1) відповідність праву на свободу думки та вираження поглядів; 2) боротьба з мовою ворожнечі є обов'язок для усіх; 3) підтримка нового покоління цифрових громадян, які зможуть розпізнавати, відкидати і протистояти мові ворожнечі в цифрову епоху; 4) скоординований збір даних і досліджень, у тому числі щодо першопричин, рушійних сил і умов, що сприяють поширенню мови ворожнечі.

Також у Стратегії визначено 13 ключових зобов'язань держав-членів у цій сфері, серед яких: 1) моніторинг та аналіз мови ворожнечі; 2) усунення першопричин, рушіїв та суб'єктів мови ворожнечі; 3) залучення та підтримка жертв мови ворожнечі; 4) скликання відповідних учасників; 5) взаємодія з новими та традиційними видами ЗМІ; 6) використання технологій; 7) використання освіти як інструменту для вирішення та протидії мові ворожнечі; 8) створення мирних, інклюзивних та справедливих суспільств для усунення першопричин і рушійних сил мови ворожнечі; 9) залучення до адвокації; 10) розробка керівництва для зовнішніх комунікацій; 11) використання партнерства; 12) розвиток навичок персоналу ООН.

Також варто зупинитися на *Кемденських принципах щодо свободи вираження поглядів та рівності*, запропонованих міжнародною правозахисною організацією Article 19, де визначено критерії, яким мають відповідати обмеження, що накладаються на право вираження поглядів

[1] United Nations Strategy and Plan of Action on Hate Speech on 18 June 2019. *United Nations*: of. website. URL: https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdf

(що змістовно дублюють ті, що викладені у МПГП); підкреслюється, що всі держави повинні розробити законодавство, що забороняє будь-яку пропаганду національної, расової чи релігійної ненависті, яка є підбурюванням до дискримінації, ворожнечі або насильства (мова ворожнечі). Робиться акцент, що держави повинні заборонити виправдовування або заперечення злочинів геноциду, злочинів проти людяності та воєнних злочинів, але лише тоді, коли такі висловлювання становлять мову ворожнечі. Також зазначається, що держави не повинні забороняти критику, спрямовану на певні ідеї або дискусії щодо них, переконань чи ідеологій, або релігій чи релігійних інституцій, за винятком випадків, коли такі висловлювання не є мовою ворожнечі тощо[1].

Щодо регіонального рівня регулювання, то згідно з позицією ЄКПЛ та ЄСПЛ мова ворожнечі не підпадає під захист ст. 10 («Свобода вираження поглядів»), що напряму випливає із принципів, закладених у ст. 14 («Заборона дискримінації») та ст. 17 («Заборона зловживання правами»).

Як і в випадку тлумачення Пакту Комітетом з прав людини, ЄСПЛ у рішенні по справі *Handyside v. the United Kingdom* зауважив, що свобода вираження поглядів застосовується не тільки до «інформації» або «ідей», що сприймаються позитивно або вважаються необразливими, але й до тих, що ображають, шокують або викликають занепокоєння держави або будь-якої групи населення. Такими є вимоги плюралізму, толерантності та широти поглядів, без яких не існує «демократичного суспільства». Це означає, серед іншого, що кожна «формальність», «умова», «обмеження» або «покарання», встановлені в цій сфері, повинні бути пропорційними законній меті, що переслідується» (§ 49)[2].

Іншими прикладами рішень щодо мови ворожнечі у практиці ЄСПЛ є Gunduz v. Turkey (№35071/97)[3], Vejdeland and others v. Sweden

[1] ARTICLE 19. The Camden principles on freedom of expression and equality. Pp. 9–10. URL: https://www.article19.org/wp-content/uploads/2009/04/Camden-Principles--ENGLISH-web.pdf

[2] Case Handyside v. the United Kingdom (Application №5493/72) on 7 December 1976. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–57499%22]}

[3] Case Gunduz v. Turkey (Application №35071/97) on 4 December 2003. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–61522%22]}

(№ 1813/07)[1], Delfi AS v. Estonia (№ 64569/09)[2], M'Bala M'Bala v. France (№ 25239/13)[3], Belkacem v. Belgium (№ 34367/14)[4], Smajic v. Bosnia and Herzegovina (№ 48657/16)[5], ROJ TV A/S v. Denmark (№ 24683/14)[6], Williamson v. Germany (№ 64496/17)[7], Lilliendahl vs Iceland (№ 29297/18)[8], Sanchez v. France (№ 45581/15)[9] тощо.

Величезну роль у розроблені політики держав-членів Ради Європи у сфері протидії антисемітизму, дискримінації, расизму, релігійної нетерпимості та ксенофобії та боротьбі з їх проявами (у т.ч. мови ворожнечі) відіграє моніторинговий орган – Європейська комісія проти расизму та нетерпимості (далі – ЄКРН), що в межах своєї компетенції видає певні рекомендації.

Так, в аспекті розуміння явища «мови ворожнечі» ЄКРН було розроблено *Загальнополітичну рекомендацію № 15 під назвою «Протидія мові ворожнечі»*. Так, під цим поняттям розробники документа розуміють «обстоювання, заохочення або підбурювання, у будь-якій формі, до приниження, ворожнечі або паплюження щодо певної особи чи групи осіб, а також будь-які вияви утиску, образ, створення

[1] Case Vejdeland and others v. Sweden (Application № 1813/07) on 9 February 2012. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–109046%22]}

[2] Case of Delfi AS v. Estonia (Application № 64569/09) on 16 June 2015. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001–155105%22]}

[3] Dieudonné M'BALA M'BALA contre la France (Requête № 25239/13) le 20 octobre 2015. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–158752%22]}

[4] Fouad Belkacem contre la Belgique (Requête № 34367/14) le 27 juin 2017. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–175941%22]}

[5] Abedin SMAJIĆ against Bosnia and Herzegovina (Application № 48657/16) on 16 January 2018. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–180956%22]}

[6] ROJ TV A/S against Denmark (Application № 24683/14) on 17 April 2018. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–183289%22]}

[7] Richard Williamson against Germany (Application № 64496/17) on 8 January 2019. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–189777%22]}

[8] Carl Jóhann Lilliendahl against Iceland (Application № 29297/18) on 12 May 2020. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001–203199%22]}

[9] Affaire Sanchez c. France (*Requête* № 45581/15) on 2 septembre 2021. *HUDOC*: of. website. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001–211599%22]}

неґативних стереотипів, стигматизації або погроз щодо такої особи чи групи осіб (і будь-яке виправдання всіх цих форм вираження) за ознакою «раси», кольору шкіри, походження, національної або етнічної належності, віку, інвалідності, мови, релігії чи вірування, статі, ґендеру, ґендерної ідентичності, сексуальної орієнтації та інших характеристик або статусу особи[1]».

Тим самим ЄКРН сформувала основні прояви такої суспільно небезпечної поведінки, окреслила коло потерпілих від неї та надала приблизний перелік захищених ознак таких осіб.

Окрім цього, у документі визначено заходи, що можна і потрібно вжити для боротьби з використанням мови ворожнечі, серед яких підвищення обізнаності про проблему (за рахунок усвідомлення важливості поваги до різноманіття у суспільстві, створення механізмів виявлення та знешкодження потенційних ділянок напруженості між членами різних громад та надання допомоги в запобіганні конфліктам і посередництво, боротьба з дезінформацією, неґативними стереотипами та стигматизацією, у тому числі через накладання чіткої заборони на профілювання тощо), надання підтримки тим, проти кого спрямована мова ворожнечі (через консультації та рекомендації, гарантування права на відшкодування шкоди та усунення перешкод, пов'язаних із цим), саморегулювання різних організацій, задіяних у просуванні такої суспільно шкідливої практики, у тому числі медіа (цей аспект може включати прийняття відповідних кодексів поведінки (або етичних кодексів) з дотриманням механізмів моніторинґу та розгляду скарг, обмін інформацією між зацікавленими суб'єктами, належне навчання тих, хто бере участь у саморегулюванні тощо), притягнення до адміністративної та цивільної відповідальності за використання мови ворожнечі, накладення адміністративних та інших санкцій проти організацій і, як крайній захід, притягнення до кримінальної відповідальності. Щодо останнього також зауважується, що у тому разі, коли національні законодавства не містять спеціальних норм, що забороняють мову ворожнечі, застосованими можуть бути

[1] Загальнополітична рекомендація ЄКРН № 15: Протидія мові ворожнечі, ухвалена 8 грудня 2015 року. Страсбург, 21 березня 2016 р. С. 3. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-hate-speech-ukrainian-tran/1680a11674

норми загального характеру, наприклад, ті, які стосуються образ. Важливим є також наявність у національних законах про кримінальну відповідальність положень, що дозволяють притягати до відповідальності за кожен з елементів, що становлять мову ворожнечі.

Окрім цього, робиться застереження, що під час вироблення відповідних спеціальних норм особливу увагу потрібно приділяти чіткому окресленню тих міркувань, які варто враховувати, вирішуючи питання про доцільність накладення кримінальних санкцій за конкретне використання мови ворожнечі. Це такі міркування: (a) чи справді існує намір підбурити до насильства, залякування, ворожості чи дискримінації або чи є ймовірність такого підбурювання; (b) чи є менш обмежувальні, але ефективні засоби реаґування на використання мови ворожнечі (такі як притягнення до відповідальності згідно з цивільним або адміністративним правом)[1].

У цій сфері діють і інші загальнополітичні рекомендації ЄКРН, серед яких:

1. Загальнополітична рекомендація ЄКРН № 5 щодо запобігання та боротьби з антимусульманським расизмом і дискримінацією від 16.03.2000 р. (переглянута 08.12.2021 р.), де зазначається, що заходи проти використання мови ворожнечі повинні слугувати захисту окремих осіб та груп осіб, а не окремих ідеологій чи релігій, а також що обмеження на мову ворожнечі не повинні використовуватися, зокрема, для придушення критики релігійних переконань. У зв'язку з цим ЄКРН підкреслює, що хоча антимусульманську риторику завжди варто засуджувати, її варт відрізняти від критики ісламу. Розрізнення цих двох понять є вкрай важливим, оскільки знищення простору для критики ісламу зашкодить демократичним дебатам і придушить свободу вираження поглядів.[2]

[1] Загальнополітична рекомендація ЄКРН № 15: Протидія мові ворожнечі, ухвалена 8 грудня 2015 року. Страсбург, 21 березня 2016 р. С. 62. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-hate-speech-ukrainian-tran/1680a11674

[2] ECRI General Policy Recommendation № 5 (revised) on preventing and combating anti-Muslim racism and discrimination adopted on 8 December 2021. Strasbourg, 2022. P. 16. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-5-revised-on-preventing-and-comb/1680a5db32

2. Загальнополітична рекомендація ЄКРН № 6 щодо боротьби з розповсюдженням расистських, ксенофобських та антисемітських матеріалів через Інтернет від 15.02.2000 р., яка стосується питань розповсюдження расистських матеріалів через інтернет і вимагає від урядів вжити необхідних заходів на національному та міжнародному рівнях для ефективної боротьби з використанням інтернету в расистських, ксенофобських та антисемітських цілях[1].

3. Загальнополітична рекомендація ЄКРН № 7 про національне законодавство щодо боротьби з расизмом і расовою дискримінацією від 13.12.2002 р. (переглянута 07.12.2017 р.), що стосується криміналізації певних форм мови ворожнечі[2].

4. Загальнополітична рекомендація ЄКРН № 9 про запобігання та протидію антисемітизмові від 25.06.2004 р. (переглянута 01.07.2021 р.), що, серед іншого, спрямована на підвищення обізнаності громадськості в контексті реституції власності єврейських осіб або громад, де це відбувається, щоб уникнути зростання антисемітських настроїв, стереотипів або мови ворожнечі[3].

5. Загальнополітична рекомендація ЄКРН № 10 щодо боротьби з расизмом і расовою дискримінацією в шкільній освіті та на її основні від 15.12.2006 р., де надаються певні заходи для боротьби з расизмом і расовою дискримінацією в школі[4].

---

[1] ECRI General Policy Recommendation № 6 on Combating the dissemination of racist, xenophobic and antisemitic materiel via the internet – adopted on 15 December 2000. Strasbourg, 2001. 8 p. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-6-on-combating-the-dissemination/16808b5a8d

[2] Загальнополітична рекомендація ЄКРН № 7 про національне законодавство щодо боротьби з расизмом і расовою дискримінацією, ухвалена 13 грудня 2002 року. 2018. 23 с. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-7-revised-on-national-legislatio/16808b5ab8

[3] Загальнополітична рекомендація ЄКРН № 9 про запобігання та протидію антисемітизмові, ухвалена 1 липня 2021 року. Страсбург, 14 серпня 2021. С. 14. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-9-revised-on-preventing-and-comb/1680a64f45

[4] ECRI General Policy Recommendation N°10 on combating racism and racial discrimination in and through school education – adopted on 15 December 2006. Strasbourg, 2008. 10 p. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-10-on-combating-racism-and-racia/16808b5ad5

6. Загальнополітична рекомендація ЄКРН №13 про боротьбу з антициганськими упередженнями та дискримінацією ромів від 24.06.2011 р., що закликає боротися з мовою ненависті, расистськими злочинами та насильством проти ромів як шляхом застосування положень кримінального законодавства, так і за допомогою превентивних заходів та заходів з підвищення обізнаності.[1]

На додаток до цього деякі питання, що стосуються використання мови ворожнечі, окреслені також у деяких інших рекомендаціях Комітету Міністрів, а також рекомендаціях та резолюціях Парламентської Асамблеї Ради Європи:

- Рекомендація № R (92) 19 Комітету міністрів державам-членам про відеоігри, що містять расизм;
- Рекомендація № R (97) 20 Комітету міністрів державам-членам щодо «мови ворожнечі»;
- Рекомендація № R (97) 21 Комітету міністрів державам-членам про ЗМІ та сприяння культурі терпимості;
- Рекомендація CM/Rec (2010) 5 Комітету міністрів державамчленам про заходи з боротьби з дискримінацією за ознаками сексуальної орієнтації або ґендерної ідентичності;
- Рекомендація 1277 (1995) про міґрантів, етнічні меншини та ЗМІ;
- Рекомендація 1543 (2001) про расизм та ксенофобію в кіберпросторі;
- Рекомендація 1706 (2005) про ЗМІ та тероризм;
- Рекомендація 1768 (2006) про створення іміджу шукачів притулку, мігрантів і біженців у ЗМ»;
- Рекомендація 1805 (2007) про блюзнірство, релігійні образи і мову ворожнечі щодо осіб на релігійному підґрунті;
- Рекомендація 2052 (2014) про протидію проявам неонацизму та правого екстремізму;

[1] Загальнополітична рекомендація ЄКРН №13: Боротьба з антициганськими упередженнями та дискримінацією ромів, ухвалена 24 червня 2011 року. Страсбург, вересень 2011. 13 с. URL: https://rm.coe.int/ecri-general-policy-recommendation-no-13-on-combating-anti-gypsyism-an/16808b5af8

- Резолюція 1345 (2003) «Про прояви расизму, ксенофобії та нетерпимості в політичній риториці»;
- Резолюція 1510 (2006) «Свобода слова й повага до релігійних переконань»;
- Резолюція 1563 (2007) «Боротьба з антисемітизмом у Європі»;
- Резолюція 1577 (2007) «На шляху до скасування кримінальної відповідальності за дифамацію»;
- Резолюція 1605 (2008) «Європейські мусульманські спільноти у протистоянні екстремізмові»;
- Резолюція 1728 (2010) «Дискримінація за сексуальною орієнтацією та ґендерною ідентичністю»;
- Резолюція 1743 (2010) «Про іслам, ісламізм та ісламофобію в Європі»;
- Резолюція 1754 (2010) «Боротьба з екстремізмом: досягнення, вади та невдачі»;
- Резолюція 1760 (2010) «Недавнє посилення риторики щодо проблем злочинності: до питання про ромів»;
- Резолюція 1846 (2011) «Боротьба з усіма формами дискримінації за релігійною ознакою»;
- Резолюція 1877 (2012) «Захист свободи слова та інформації в інтернеті та інтернет ЗМІ»;
- Резолюція 1928 (2013) «Ґарантії прав людини у зв'язку з релігійними й іншими переконаннями та захист релігійних громад від насильства»;
- Резолюція 1948 (2013) «Припинення дискримінації за ознакою сексуальної орієнтації та ґендерної ідентичності»;
- Резолюція 1967 (2014) «Стратегія профілактики расизму та нетерпимості в Європі»;
- Резолюція 2011 (2014) «Протидія проявам неонацизму та правого екстремізму»;
- Резолюція 2069 (2015) «Розпізнавання і попередження неорасизму» тощо.

Щодо законодавства ЄС з цього приводу, то на відміну від ініціатив Ради Європи, воно є фрагментарним та недостатньо розробленим.

Так, основоположними у досліджуваній проблематиці є ст. 10 («Свобода думки, совісті та релігії»), ст. 11 («Свобода вираження поглядів та інформації»), 21 («Недискримінація») *Хартії ЄС*[1].

Базовим документом у цьому відношенні є також *Рамкове рішення 2008/913/ЈНА про боротьбу з певними формами та проявами расизму та ксенофобії засобами кримінального права від 28.11.2008 р.*, що спрямоване на забезпечення того, щоб правопорушення, пов'язані з расизмом і ксенофобією, підлягали ефективному, пропорційному і стримуючому кримінальному покаранню[2], а також інші антидискримінаційні положення, серед яких *Директива Ради 2000/43/ЄС від 29.06.2000 р. про впровадження принципу рівного ставлення до осіб незалежно від расового чи етнічного походження*[3] *та Директива Ради 2000/78/ЄС від 27.11.2000 р., що встановлює загальні рамки рівного ставлення у сфері зайнятості та професійної діяльності*.[4]

Особлива увагу на рівні ЄС приділяється і протидії конкретним формам мови ворожнечі та злочинів на ґрунті ненависті, з якими стикаються групи та спільноти. Мова йде про такі стратегічні документи як *Стратегія ЄС щодо боротьби з антисемітизмом та сприяння єврейському життю (2021-2030)* від 05.10.2021 р.[5], *Стратегіч-*

---

[1] Charter of Fundamental Rights of the European Union (2000/C 364/01). *Official Journal of the European Communities*, 18.12.2000. C 364/3. 22 p. URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[2] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0913

[3] Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0043

[4] Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078

[5] About the EU strategy. EU Strategy on combating antisemitism and fostering Jewish life (2021–2030). *European Commission:* of website. URL: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/combating-antisemitism/eu-strategy-combating-antisemitism-and-fostering-jewish-life-2021-2030/about-eu-strategy_en

ні рамки ЄС для ромів щодо рівності, інтеграції та участі на 2020–2030 роки від 07.10.2020 р.[1] *тощо.*

Застосованою до цієї сфери є і Директива про права жертв від 25.10.2012 р., яка встановлює мінімальні стандарти щодо прав, підтримки та захисту всіх жертв злочинів, приділяючи особливу увагу жертвам, які постраждали від злочину, вчиненого з упередженим або дискримінаційним мотивом.[2]

Окреме місце у досліджуваній царині займає вищезгадана *Директива про аудіовізуальні медіа-послуги від 10.03.2010 р.*, яка забороняє підбурювання до ненависті в аудіовізуальних медіа-послугах і просування дискримінації в аудіовізуальних комерційних комунікаціях.[3]

Заслуговують на увагу і положення *Кодексу поведінки щодо протидії незаконній мові ворожнечі в Інтернеті від 31.05.2016 р.*, що заохочує швидке та ефективне видалення незаконного контенту з мовою ворожнечі та сприяє співпраці між онлайн-платформами, громадянським суспільством та органами державної влади[4].

Тут також варто підкреслити, що певний позитивний зсув у питанні регламентації мови ворожнечі на рівні ЄС, може бути здійснений

---

[1] A Union of Equality: EU Roma strategic framework for equality, inclusion and participation {SWD(2020) 530 final}. *European Commission:* of website. URL: https://commission.europa.eu/system/files/2021–01/eu_roma_strategic_framework_for_equality_inclusion_and_participation_for_2020_-_2030_0.pdf

[2] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012L0029&qid=1699218089896

[3] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010L0013&qid=1699218089896

[4] The EU Code of conduct on countering illegal hate speech online. The robust response provided by the European Union. *European Commission:* of website. URL: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

у зв'язку із прийняттям *пропозиції Європейської конвенції від 09.12.2021 р.* щодо розширення переліку злочинів, викладеного у ст. 83(1) ДФЄС, за рахунок мови ворожнечі та злочинів на ґрунті ненависті[1].

Отже, з приводу вищевикладеного підкреслимо, що інформаційний простір, як середовище, де створюється, обробляється, зберігається та поширюється інформація, стикається з різними загрозами, що можуть мати далекосяжні наслідки як на рівні окремих осіб, суспільств, держав, так і всього міжнародного континууму. Пропаганда війни, дезінформація та мова ворожнечі часто виступають як тактики, що сприяють соціальному поділу, підриву довірі та ескалації напруженості. Подолання цих загроз вимагає розвинутої законодавчої регламентації, а також комплексного підходу за участі національних урядів, громадянського суспільства, технологічних компаній та розвинутого міжнародного співробітництва. При цьому розробка стратегій боротьби з цими деструктивними проявами інформаційного простору вимагає дотримання справедливого та складного балансу між шкодою, яку вони заподіюють (або можуть заподіяти), та свободою слова як гарантією демократичного розвитку.

1.4. CAN SPAM Act як приклад прагматичного підходу кримінально-правової охорони суспільних відносин інформаційної безпеки

Проблема кримінально-правового регулювання в сфері інформаційної безпеки має ще один вимір. Небезпека посягань очевидна, необхідність гідної кримінально-правової реакції безсумнівна. Водночас інформаційна безпека є однією з найбільш динамічних сфер діяльності людини. Збільшення зайнятості в сфері ІТ є загальновиз-

[1] A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime: Communication from the Commission to the European Parliament and the Council. *EUR-lex*: of website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0777

наним трендом та прогнозом ринку праці. Зрозуміло, що кримінально-правове регулювання має враховувати цю особливість. Прикладом тут може слугувати протидія розповсюдженню спаму (SPAM, sending of predatory and abusive e-mail)[1]. Спам визначається як розсилка масових повідомлень електронної пошти, які мають рекламний, порнографічний або інший небажаний характер. В окремих випадках – повідомлення для подальшого вчинення шахрайства. Суттєвою ознакою спаму є те, що отримувачі такі листи не замовляли чи не можуть відмовитися від їх подальшого отримання.

Отже, розповсюдження спаму, як правило, полягає в надсиланні великій кількості адресатів повідомлень, що вони не замовляли. Суспільна небезпечність такого діяння має певну специфіку. З точки зору конкретного користувача матеріальні збитки від розповсюдження спаму незначні, вони врешті-решт зводяться до оплати інтернет-послуг, пов'язаних з отриманням зайвої кореспонденції. Однак з точки зору провайдерів, організацій, що надають послуги доступу до інтернету, спам є досить небезпечним явищем, оскільки його наявність створює зайве, некорисне навантаження обладнання й ускладнює роботу інформаційної системи. Ще одним показником суспільної небезпечності спаму є втрати робочого часу працівників підприємств, установ та організацій, які використовують інтернет у своїй роботі.

Стаття 363[1] КК України передбачає відповідальність за масове розповсюдження повідомлень електрозв'язку. Кримінальна відповідальність у разі вчинення таких дій настає тільки тоді, коли спричинено наслідки у вигляді порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Проте, розповсюдження спаму, як правило, не призводить до таких наслідків[2]. Ситуація, коли в результаті масового розповсюдження повідомлень електрозв'язку настають зазначені наслідки, є винятковою. Пору-

---

[1] Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : моногр. МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка.Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 453-465.

[2] Музика А. А., Азаров Д. С. Законодавство України про відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. К.: Вид. Паливода А. В., 2005. С. 79.

шення або припинення роботи засобів опрацювання інформації варто віднести до абсолютно нетипових наслідків розповсюдження спаму. Отже, маємо констатувати, що інформаційні суспільні відносини через недосконалість статті 363[1] КК України практично не захищені від посягань, пов'язаних із розповсюдженням спаму. «Звичайне» розповсюдження спаму не можна кваліфікувати за цією нормою, оскільки воно не призводить до наслідків, зазначених у статті 363[1] КК. Тому до недоліків чинного кримінального законодавства треба віднести і його недостатню ефективність у протидії такій загрозі, як спам.

Водночас необхідно зауважити, що діяльність із масового розповсюдження повідомлень електрозв'язку не може однозначно розглядатися як суспільно небезпечна. Направлення рекламних повідомлень у соціальних мережах, через сервіси електронної пошти є звичайною практикою сучасного бізнесу, є важливим та перспективним полем рекламної діяльності. Велика кількість рекламних компаній, маркетингові підрозділи торгівельних мереж постійно працюють над встановленням контактів клієнтів, з'ясуванням видів товарів та послуг, які їх цікавлять, підготовкою та надсиланням клієнтам рекламних пропозицій.

Враховуючи зазначене, представляє інтерес аналіз одного з найбільш прогресивних в цій сфері законодавчих актів, Федерального Закону Сполучених Штатів Америки від 16.12.2003 р. Controlling the Assault of Non-Solicited, Pornography and Marketing Act (U. S. A. CAN-SPAM Act)[1].

Перед тим як перейти до розгляду ознак складів злочинів, передбачених цим нормативним документом, необхідно зробити деякі термінологічні уточнення. Предметом передбачених законом злочинів є комерційні повідомлення електронної пошти (commercial electronic mail message), що визначаються як повідомлення електронної пошти, головною метою яких є комерційна реклама або пропозиція конкретних товарів чи послуг (включаючи зміст платних інтернет-сайтів). При цьому в законі зазначається, що до комерційної пошти не відносяться

[1] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). Public Law 108–187. U. S. *Government Publishing Office*: of. website. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

повідомлення про трансакції або відносини (transactional or relationship message). Останні являють собою повідомлення, метою яких є:

1) підтвердження комерційної трансакції отримувача; 2) повідомлення про гарантійне чи сервісне обслуговування продуктів або послуг, придбаних отримувачем; 3) повідомлення отримувача про статус або баланс його фінансового рахунку чи про іншу подібну інформацію стосовно позик, триваючих комерційних відносин тощо; 4) забезпечення отримувача інформацією щодо його трудових відносин; 5) забезпечення отримувача інформацією про доставку замовлених ним товарів чи послуг.

Важливим для формулювання ознак досліджуваних складів злочинів є також термін «header information», який можна перекласти як «інформація, що міститься в заголовку повідомлення». До цих відомостей CAN-SPAM Act відносить дані стосовно джерела, призначення та маршрутизації електронного листа,а також будь-які інші дані, що дозволяють ідентифікувати особу, яка «ініціювала» повідомлення. Ініціювання повідомлення визначається як його передавання, спричинення початку процесу передавання або забезпечення виконання подібних дій іншими особами. Метою такого складного формулювання є виключення зі сфери дії закону провайдерів інтернет-послуг, що здійснюють транспортування передачі (routine conveyance) – передачу, маршрутування, ретрансляцію, керування або зберігання шляхом автоматичного технічного процесу повідомлень електронної пошти, для яких інші особи визначили адреси отримувачів. Транспортування передачі не є ініціюванням повідомлення за визначенням, закон розділяє ці поняття для того, щоб ідентифікувати діяльність саме відправника повідомлень, відокремити її від роботи провайдера послуг інтернет, який забезпечує фактичне передавання повідомлення.

Також закон оперує терміном «захищений комп'ютер» (protected computer), він визначається у федеральному законі щодо захисту національної інфраструктури (U. S. National Information Infrastructure Protection Act of 1996)[1]. До захищених відносяться: 1) комп'ютери, які використовуються фінансовими установами або урядом США

[1] U. S. National Information Infrastructure Protection Act of 1996. *Electronic privacy information center*: website. URL: http://epic.org/security/1996_computer_law.html

виключно або від їх імені чи для виконання їх завдань, і діяння, яке утворює злочин, чинить вплив на таке використання; 2) комп'ютери, які використовуються в комерційній або комунікаційній діяльності, що здійснюється між штатами або на міжнародному рівні, включаючи комп'ютери, що перебувають поза межами США, які використовуються у спосіб, що впливає на таку комерційну або комунікаційну діяльність.

Нарешті «множинними» (multiple) повідомлення варто уважати тоді, коли їх кількість перевищує 100 за 24 години, 1000 – протягом 30 днів чи 10000 – протягом року.

Отже, відповідно до CAN-SPAM Act діяння, вчинені під час комерційної діяльності, що відбувається між штатами або є міжнародною, або діяння, вчинені для забезпечення такої діяльності третіх осіб, треба вважати федеральними злочинами, коли вони становлять:

1) несанкціонований доступ до захищеного комп'ютера та умисне ініціювання передачі множинних комерційних повідомлень електронної пошти з такого комп'ютера або через нього (18 U. S. C. 1037 (a)(1));

2) використання захищеного комп'ютера для передавання або перенаправлення комерційних повідомлень електронної пошти з метою введення в оману отримувачів або інтернет-провайдерів стосовно джерела таких повідомлень (18 U. S. C. 1037 (a)(2));

3) істотне викривлення інформації, що міститься в заголовку множинного повідомлення, та умисне ініціювання передавання таких повідомлень (18 U. S. C. 1037 (a)(3))

4) реєстрацію з використанням істотно викривленої інформації стосовно ідентифікації особи, що реєструється, п'яти або більше облікових записів електронної пошти чи облікових записів мережевих користувачів, або двох чи більше доменних імен та умисне ініціювання передавання множинних комерційних повідомлень електронної пошти з будь-якої комбінації таких облікових записів або доменних імен (18 U. S. C. 1037 (a)(4));

5) представлення себе шляхом обману особою або законним представником особи, на яку зареєстровано п'ять або більше IP-адрес (цифрових ідентифікаторів певних комп'ютерів в мережі Інтернет),

та умисне ініціювання передачі множинних комерційних повідомлень електронної пошти з таких адрес (18 U. S. C. 1037 (a)(5)).

Закон передбачає такі кваліфікуючі ознаки перелічених посягань:

1) вчинення означених дій для подальшого здійснення злочину, передбаченого федеральним законодавством або законами певного штату; 2) вчинення означених злочинів після вчинення будь-якого з посягань, передбачених розд. 1030 Зводу законів США (федеральний кримінальний закон про «комп'ютерні» злочини), або будь-якого злочину, передбаченого законодавством певного штату, пов'язаного з передачею множинних комерційних повідомлень електронної пошти або несанкціонованим доступом до комп'ютерної системи; 3) вчинення злочину, передбаченого U. S. C. 1037 (a)(4) з використанням більш ніж 20 облікових записів електронної пошти або облікових записів мережевих користувачів або більш ніж 10 доменних імен, реєстрація яких пов'язана з фальсифікацією; 4) вчинення множинного розсилання в розмірі 2500 листів за день або 25 000 за 30 днів, або 2 500 000 листів за рік; 5) втрати однієї або більше осіб унаслідок вчинення означених злочинів складають 5000 $ США або більше протягом одного року; 6) у результаті вчинення означених злочинів особа, яка його вчинила, отримала протягом одного року майно або будь-які майнові переваги, сума яких у грошовому вираженні дорівнює або перевищує 5000 $ США; 6) означені злочини було вчинено групою осіб і винна особа виконувала роль організатора або керівника.

Як приклад застосування норм цього закону розглянемо кваліфікацію масового розсилання повідомлень електронної пошти, запропоновану в обвинувальному вироку по справі США проти Роберта Соловея та Ньюпорт Інтернет Маркетинг (USA v. Robert Alan Soloway and Newport Internet Marketing Corporation)[1]. Головною метою діяльності обвинуваченого було отримання майна шляхом обману. Для цього Роберт Соловей розмістив на багатьох сайтах рекламу програмного забезпечення та послуг створеної ним корпорації Ньюпорт

[1] Idictment USA v. Robert Alan Soloway and Newport Internet Marketing Corporation. *Mortgagespam site*: website. URL: http://www.mortgagespam.com/soloway/Indictmentfiled.pdf

Інтернет Маркетинг. Ці послуги полягали в організації законної розсилки масової реклами через електронну пошту. Проте інформація про наявність легально отриманих адрес електронної пошти у базі даних, ефективність запропонованого програмного забезпечення, наявність цілодобової технічної підтримки та гарантованого повернення вартості програмного забезпечення у випадку невиправданого прибутку не відповідали реальності. Крім того, Роберт Соловей, використовуючи незаконно здобуті електронні адреси, здійснював масову розсилку комерційних повідомлень електронної пошти, пропагуючи послуги та програмні продукти компанії «Ньюпорт Інтернет Маркетинг». За даними обвинувачення, таких повідомлень налічувалися десятки мільйонів. При цьому адреси, які він використовував для фальсифікації реального джерела повідомлень, належали, як правило, тим особам, які внаслідок введення в оману придбали рекламоване ним програмне забезпечення. Приховування джерела повідомлень здійснювалося з використанням спеціального програмного забезпечення, яким він фальсифікував дані заголовків повідомлень. Така фальсифікація чинилася шляхом залишення поля «Звідки» (From) порожнім або заповнення його неіснуючою адресою чи адресою, що належала іншій особі. Також для приховування реальної адреси відправника Роберт Соловей використовував близько 2000 так званих проксі-серверів (proxy servers) спеціальних мережевих служб, які дозволяють переадресовувати та перенаправляти потоки електронної пошти та змінювати відомості про джерело повідомлення. Обвинувачення детально описує збитки, завдані внаслідок розсилання масових повідомлень електронної пошти. У даному випадку вони головним чином пов'язані з ускладненнями легального використання електронної пошти особами, чиї електронні адреси використовував зловмисник. У деяких випадках це призводило до припинення обслуговування електронних адрес цих осіб провайдерами інтернет-послуг. Провайдери інтернету мають право приймати такі рішення, оскільки масове розсилання є порушенням загальних правил надання доступу до мережі. Отже, реальні володарі адрес, які використовував Роберт Соловей, несли відповідальність за розсилання, що він організовував. Для тих із них, хто здійснює господарську діяльність в ін-

тернеті, подібні заходи завдавали істотних збитків. В інших випадках володарі використовуваних злочинцем адрес отримували на свої електронні поштові скриньки численні повідомлення про те, що пошту не доставлено (у тих випадках, коли програма Роберта Соловея надсилала листи на ті адреси, які вже не існували). Ці повідомлення були численними, займали багато місця на серверах, а їх видалення спричинило втрати як часу, так і грошей.

У контексті досліджуваного закону дії Роберта Соловея були кваліфіковані як використання захищеного комп'ютера (такими в цій справі були сервери крупних провайдерів та проксі-сервери, що використовувалися для організації зв'язку між штатами) для передавання або перенаправлення комерційних повідомлень електронної пошти з метою введення в оману отримувачів стосовно джерела таких повідомлень (18 U. S. C. 1037 (a)(2)), а також як істотне викривлення інформації, що міститься в заголовку множинного повідомлення, та умисне ініціювання передавання таких повідомлень (18 U. S. C. 1037 (a)(3)). Крім цього, йому були інкриміновані шахрайство, крадіжка ідентифікаційних відомостей та відмивання грошей.

Цей приклад надає переконливі аргументи для визначення суспільної небезпечності поширення спаму. Використовуючи його як інструмент для вчинення інших злочинів або як форму недобросовісної реклами, зловмисники завдають наслідки у сфері використання інформаційних технологій. Ці наслідки виявляються в суттєвому ускладненні або навіть повній неможливості користуватися електронною поштою. У такий спосіб, суспільна небезпека, яка виникає внаслідок поширення спаму як самостійної атаки на використання інформаційних технологій, оцінюється за збитками, які завдаються особам через ці ускладнення або неможливість використання електронної пошти.

CAN-SPAM Act не обмежується засобами кримінально-правового впливу на суспільні відносини, він передбачає також інші заходи правового захисту для осіб, які використовують комерційну електронну пошту (Sec. 5. Other protections for users of commercial electronic mail). Якщо перелічені вище діяння відносяться до 18 титулу Зводу Законів США, який має назву «Злочини та Кримінальний процес»,

то норми, що передбачають інші заходи правового захисту, відносяться до 15 титулу «Комерція та торговельна діяльність». Такі заходи полягають у встановленні ознак діянь, які варто вважати незаконними та за вчинення яких, відповідно, може наставати цивільна або господарська відповідальність. Ці діяння поділяються на дві групи: вимоги до передачі сигналів (Requirements for transmition of messages); кваліфіковані порушення,що відносяться до комерційної електронної пошти (Aggravated violations relating to commercial electronic mail).

До діянь першої групи закон відносить:

1) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти або повідомлень про трансакції чи відносини, які містять істотно сфальсифіковану інформацію в заголовку або таку інформацію заголовку, що вводить в оману (під останньою розуміється інформація, яка є технічно правильною, тобто листи дійсно відправлялися з адреси, яка в них зазначена, але можливість надсилання листів з цієї адреси отримана шляхом обману, наприклад, через використання троянської програми) (15 U. S. C. 7704 (a)(1));

2) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, що містить опис предмета (subject heading), сформульований таким чином, щоб ввести в оману отримувача (15 U. S. C. 7704 (a)(2));

3) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, яке не містить посилання на функціонуючу електронну адресу чи інший подібний механізм, що дозволяє відмовитися від подальшого отримання подібної кореспонденції (15 U. S. C. 7704 (a)(3));

4) ініціювання передачі комерційного повідомлення електронної пошти особі, яка в установленому порядку відмовилася від отримання подібної кореспонденції (15 U. S. C. 7704 (a)(4));

5) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, яке не містить чіткої та зрозумілої вказівки на те, що повідомлення є рекламою або особа має можливість відмовитися від отримання такої кореспонденції в подальшому або без вказівки на дійсну фізичну поштову адресу відправника (15 U. S. C. 7704 (a)(5)).

До кваліфікованих порушень, таких, що мають обтяжуючі ознаки, належать:

1) так звані «атаки збору врожаю» та «словникові атаки» (address harvesting and dictionary attacks), які полягають у використанні для розсилання електронних адрес, отриманих шляхом автоматизованої обробки сайтів, у інформаційному наповненні яких спеціально зазначається, що особа, котра оперує сайтом, не надає, не продає, не передає іншим чином представлені на сайті електронні адреси для надсилання на них комерційної інформації, або у використанні для розсилання електронних адрес, отриманих у результаті автоматизованого підбору та перестановок імен, символів, цифр тощо (15 U. S. C. 7704 (b)(1));

2) створення множинних облікових записів електронної пошти для подальшого розсилання комерційних повідомлень електронної пошти шляхом використання засобів автоматизації (15 U. S. C. 7704 (b)(2));

3) ретрансляція повідомлень електронної пошти або повідомлень про трансакції чи відносини, які містять істотно сфальсифіковану інформацію в заголовку або таку інформацію заголовку, що вводить в оману через захищений комп'ютер, доступ до якого отримано несанкціоновано (15 U. S. C. 7704 (b)(3));

4) направлення без спеціального маркування комерційних повідомлень електронної пошти, які містять відомості сексуального характеру, на захищений комп'ютер (15 U. S. C. 7704 (b)(4)).

Прикладом застосування цих засобів правової охорони суспільних відносин у сфері використання електронної пошти може слугувати судове рішення в широковідомому цивільному процесі соціальної мережі Facebook проти так званого «короля спаму» Сенфорда Уоллеса та його спільників. Відповідно до рішення окружного суду Північного округу Каліфорнії Уоллес був зобов'язаний виплатити компенсацію позивачеві в розмірі 710 737 650 доларів США[1]. Аналіз позовної заяви

[1] Default Judgment in favor of Facebook, Inc. against Sanford Wallace. Signed by Judge Jeremy Fogel on 10/29/2009. *The Justia Federal District Court Filings & Dockets site*: website. URL: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2009cv00798/211911/92/

в цій справі дає можливість установити, що свої матеріальні претензії Facebook обґрунтовувала в тому числі й порушенням норм досліджуваного закону, які об'єднані в розглянутому вище розділі. Зокрема, працівники Facebook наголошували, що Уолес активно розсилав небажаний комерційний контент серед користувачів платформи. Його метод полягав у тому, що він незаконно використовував облікові записи інших клієнтів Facebook для відправлення таких повідомлень. Оскільки обмін повідомленнями в соціальних мережах можливий лише за взаємною згодою користувачів, дії Уолеса викликали ситуацію, коли клієнти отримували рекламні повідомлення, які нібито надсилалися їхніми друзями чи колегами. Таким чином, використовуваний Уолесом механізм поширення спаму суттєво ускладнював його виявлення, завдаючи шкоду користувачам платформи і викликаючи втрату репутації та довіри до Facebook. У позовній заяві дії Уолеса були представлені також як направлення на захищений комп'ютер повідомлень комерційного характеру із заголовками, що вводять в оману (15 U. S. C. 7704 (a) (1)); ініціювання передачі на захищений комп'ютер комерційного повідомлення, що містить оманливий опис предмета (15 U. S. C. 7704 (a) (2)); ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, яке не містить посилання на функціонуючу електронну адресу чи інший подібний механізм, що дозволяє відмовитися від подальшого отримання подібної кореспонденції (15 U. S. C. 7704 (a)(3)), тощо[1].

Здійснений огляд федерального закону США щодо регулювання відносин у сфері користування комерційною електронною поштою дає змогу зробити кілька важливих висновків.

По-перше, особливу увагу американський законодавець приділяє правовому регулюванню саме комерційної електронної пошти. У такий спосіб вирішується дуже важлива проблема протидії спаму. На за-

[1] Complaint against Sanford Wallace, Adam Arzoomanian, Scott Shaw (Filing fee $ 350.00, receipt number 54611004760.). Filed byFacebook, Inc.. (gm, COURT STAFF) (Filed on 2/24/2009) (Additional attachment(s) added on 3/5/2009: # 1 Civil Cover Sheet) (gm, COURT STAFF). *The Justia Federal District Court Filings & Dockets site:* website. URL: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2009cv00798/211911/1/0.pdf

конодавчому рівні фіксується класифікація нормативних підходів до масових розсилань залежно від їх змісту. Якщо шляхом масового розсилання здійснюється розповсюдження комп'ютерних вірусів, порнографії чи створюються умови для подальшого вчинення шахрайства, таке розсилання однозначно визнається злочинним і отримує правову оцінку в контексті відповідних законів. Це положення фіксується CAN-SPAM Act у параграфі (c) четвертого розділу. У той же час, якщо розсилання масових повідомлень визнається розповсюдженням рекламних повідомлень, дії осіб, які його здійснюють, визнаються суспільно небезпечними лише у випадку порушення встановлених правил використання комерційної електронної пошти. Цей нормативний акт враховує вищезазначену особливість спаму, яка полягає в тому, що він у певних формах може бути корисним суспільним явищем. Такий регуляторний підхід сприяє забезпеченню балансу між позитивними та негативними наслідками криміналізації. Саме тому даний нормативно-правовий акт сприяє цивілізованому розвитку суспільно корисного сегменту спаму.

По-друге, у питанні регулювання спаму американський законодавець обрав модель «opt-out», вважаючи, що відправник повідомлень повинен чесно інформувати отримувачів про зміст та джерело повідомлень, а отримувачі, у свою чергу, повинні мати можливість відмовитися від подальшого отримання подібної кореспонденції від конкретного відправника. Існує інша модель, відома як «opt-in», яка є більш жорсткою. Згідно з нею, легальним є лише масове розсилання на електронні адреси отримувачів, які заздалегідь виразили своє бажання отримувати таку кореспонденцію.

По-третє, в рамках встановленого американським законодавством підходу, до критеріїв суспільної небезпечності масового розсилання комерційних повідомлень електронною поштою слід відносити: незаконне використання захищених комп'ютерів або їх використання для обману отримувачів; маніпуляцію реквізитами електронних листів для унеможливлення ідентифікації відправника; використання для масового розсилання електронних листів адрес або доменних імен, які були зареєстровані з використанням фальсифікованих даних (у таких випадках реквізити листів залишаються незмінними, проте не-

можливість ідентифікації відправника забезпечується спотворенням даних щодо реєстрації джерела повідомлень); використання чужих IP-адрес для масового розсилання від власного імені.

По-четверте, CAN-SPAM Act пропонує розгалужену систему кваліфікуючих ознак розповсюдження множинних повідомлень комерційного зв'язку. Серед них на окрему увагу заслуговує механізм визначення розміру шкоди, заподіяної масовим розповсюдженням повідомлень електронної пошти, та розміру прибутку, отриманого шляхом учинення злочинів, передбачених досліджуваним законом. Ці ознаки розглядаються в контексті певного проміжку часу. Наприклад, множинне розсилання вважатиметься кваліфікованим не просто тоді, коли злочином заподіяно шкоду в розмірі 5250 доларів, а тоді, коли сума всіх втрат потерпілого, пов'язаних з множинним розсиланням певної особи, склала понад 5000 доларів за один рік. Як видається, таке законодавче рішення найповніше відображає специфіку заподіяння шкоди від спаму. Вона, як правило, складається з великої кількості незначних втрат, які, отримуючи системний характер, із часом набувають значення, достатнього для правової оцінки.

По-п'яте, для розв'язання, або, використовуючи влучний термін з назви закону, контролювання проблеми комерційного спаму американський законодавець не обмежується нормами про кримінальну відповідальність. З метою комплексного нормативно-правового впливу, закон встановлює вимоги до оформлення комерційної електронної кореспонденції, прозорості механізму зв'язку з відправником та можливості відмовитися від подальшого отримання подібних повідомлень, а також законність збирання електронних поштових адрес та інше. Порушення цих вимог може призвести до цивільної відповідальності для відправника повідомлень. Важливою особливістю, яка відрізняє злочини, передбачені законом CAN-SPAM Act, від цивільно-правових правопорушень, є масовість розсилання. Таким чином досягається вирішення проблеми відповідності інтенсивності правового впливу ступеню небезпеки конкретного порушення.

Отже, правове регулювання масового розповсюдження повідомлень електрозв'язку відповідає соціальному контексту та значенню цього явища в тому випадку, коли виконуються наступні умови: 1) масове розповсюдження повідомлень електрозв'язку не розглядається однозначно як протиправна діяльність; 2) на рівні нормативно-правових актів встановлюються правила для проведення таких розсилань як конкретного виду господарської діяльності; 3) комплекс правових заходів для протидії негативним наслідкам масових розсилань включає норми, які передбачають відповідальність за порушення цих правил; 4) диференціація цих правових заходів здійснюється в залежності від ступеня суспільної небезпечності наслідків масового розповсюдження вказаних повідомлень.

В контексті цього розглянемо, як регулюється діяльність щодо розповсюдження спаму, нормами національного законодавства. У Правилах надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 11.04.2012 р. № 295[1], під спамом розуміються електронні, текстові та/або мультимедійні повідомлення, які без попередньої згоди (замовлення) абонента, оператора, провайдера умисно та/або масово надсилаються на їх адреси електронної пошти або кінцеве обладнання, крім повідомлень оператора, провайдера щодо надання телекомунікаційних послуг або органів державної влади у випадках, передбачених законодавством. Правила містять норми щодо порядку надання та використання інтернет-послуг, серед яких наявні заборони замовляти, пропонувати розсилання або розсилати спам. Крім цього забороняється використовувати мережеві ідентифікатори інших осіб, фальсифікувати мережеві ідентифікатори, використовувати неіснуючі мережеві ідентифікатори.

Тобто в загальних рисах українське законодавство містить норми, подібні до розглянутого американського закону. Разом із тим, слід визнати, що на рівні матеріальних норм, які стосуються регу-

[1] Про затвердження Правил надання та отримання телекомунікаційних послуг: Постанова Кабінету Міністрів України № 295 від 11.04.2012. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/295–2012-%D0%BF#n8

лювання порядку надання й отримання телекомунікаційних послуг, українське законодавство є значно жорсткішим ніж американське. Якщо останнє в певних випадках дозволяє розсилання кореспонденції, яку не замовляв отримувач, то національне її однозначно забороняє. Національне законодавство об'єднує два вищеназвані підходи до регулювання спаму, установлюючи одночасну заборону двох типів: як «opt in», так і «opt out». Однак засобів забезпечення цих вимог українське законодавство не містить.

Уявімо, що Роберт Соловей розпочав свою діяльність в Україні. Хоча до нього можна було б застосувати норми, пов'язані із відповідальністю за шахрайство та відмивання грошей, відносно порушення суворих національних вимог щодо розповсюдження спаму та юридичної оцінки наслідків його діяльності українська юстиція мала б виявити невизначеність. Фактично, його ініційована розсилка стала б порушенням вже згаданих Правил надання та отримання телекомунікаційних послуг: надіслані повідомлення не містили достовірної інформації про відправника, отримувачі не замовляли їх і не мали можливості відмовитися від них. Проте відповідальність за порушення цих правил настає тільки в разі «здійснення дій, що призвели до зниження якості функціонування телекомунікаційних мереж» (ст. 148^1 КпАП України). Такі наслідки не були властиві діяльності Соловея. Навпаки, реальні небезпечні наслідки були пов'язані з тим, що через функціонування мережі в режимі масового розповсюдження повідомлень ускладнювалося користування електронною поштою. Використання ст. 363^1 КК України в цьому випадку теж було б неможливим, оскільки наслідки, що характеризували діяльність Соловея, не призводили до «порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку».

Крім цього, розгляд ст. 363^1 КК у контексті нормативних вимог до надання чи отримання телекомунікаційних послуг дозволяє встановити ще одну ваду цієї норми. Суть проблеми заключається в тому, що кримінальний закон не відповідає матеріальним нормам, що визначають правила користування послугами з відправлення повідомлень.

Оскільки передбачене цією нормою кримінальне правопорушення визначається як масове розповсюдження повідомлень електрозв'язку без попередньої згоди адресатів, то випадки масового розсилання замовлених повідомлень, які, проте, містять викривлені дані про відправника або не надають можливості відмовитися від подальшого отримання, не вважатимуться ознакою кримінального діяння, навіть якщо такі дії заборонені Правилами отримання телекомунікаційних послуг. Іншими словами, несумісність матеріальних та охоронювальних норм призводить до неефективності правового регулювання даної сфери суспільних відносин.

У той же час, вимоги національного законодавства щодо проведення масових розсилань, зокрема заборона відсилання повідомлень без попереднього замовлення отримувача, хоч і не підтримуються відповідними санкційними нормами, мають негативне значення. Наявність таких обмежень обмежує можливість розвитку відповідних галузей господарської діяльності, роблячи їх правове поле значно меншим. Ті види комерційної діяльності, яким американський законодавець намагається сприяти та розвивати для підвищення рівня національної економіки, відповідно до нашого законодавства стають неможливими через безумовну заборону.

Таким чином, для вирішення проблеми кримінальної відповідальності за розсилання масових телекомунікаційних повідомлень перш за все необхідно встановити чіткі правила здійснення подібної діяльності.Доцільно, щоб ці правила охоплювали не лише електронну пошту, але й інші засоби зв'язку, такі як, наприклад, смс-повідомлення, повідомлення у соціальних мережах тощо. В той же час ми вважаємо, що зміст нормативних вимог не повинен бути настільки суворим, як це передбачає чинне законодавство. Нормативні положення повинні стимулювати і надавати можливості для розвитку легального масового розсилання повідомлень електрозв'язку, оскільки світова практика свідчить про його важливість для економіки країни як каналу доставки інформації користувачам товарів і послуг. За порушення цих правил доцільно передбачити кримінальну відповідальність.

Висновки

1. Інформаційну безпеку розглянуто як систему суспільних відносин щодо забезпечення реалізації інформаційної потреби громадян, суспільства, держави. Структуру інформаційної безпеки складають відносини в сфері використання інформаційних технологій, відносини в сфері забезпечення доступу до інформації та відносини в сфері формування інформаційного ресурсу. Кожному з названих елементів інформаційної безпеки властиві специфічні проблеми кримінально-правової охорони. Для використання інформаційних технологій це – примітивізація з метою протиправного застосування новітніх технологій. Для забезпечення доступу до інформації – надмірна розгалуженість та неузгодженість заборон. Для формування інформаційного ресурсу – визначення меж кримінально-правового впливу. Друга означена проблема, як видається, має локальний характер, її ефективне розв'язання цілком можливе в межах національного правового дискурсу. Водночас розв'язання першої та третьої потребують аналізу наявного зарубіжного та міжнародного досвіду.

2. Проведено аналіз міжнародних стандартів, рекомендацій ЄС щодо протидії «кіберзлочинам». Зокрема, Конвенції ЄС про кіберзлочинність від 23.11.2001 р. та Директиви Європейського парламенту і ради ЄС 2016/1148 від 06.07.2016 р. про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. Варто зазначити, що більшість кримінальних правопорушень, які визначені цим документом, закріплені в КК України. Що стосується Директиви Європейського парламенту і ради ЄС, то розглянуто питання, пов'язані із необхідністю виконання окремих положень державою для ефективної протидії правопорушенням, що вчиняються у цій сфері.

3. Зауважено, що криміногенний вплив появи та розширення сфери протиправного застосування віртуальних активів міжнародною професійною спільнотою розглядається як такий, що в меншій мірі потребує змін кримінального законодавства, але актуалізує завдання правового регулювання обігу віртуальних активів на національному

рівні. Крім того, важливою проблемою визнається організаційно-технічний рівень готовності правоохоронних органів протидіяти злочинному використанню віртуальних активів.

4. Зазначено, що сучасна міжнародна дискусія щодо правового регулювання соціалізації ШІ характеризується більшою увагою до практичних проблем. Правове регулювання використання технологій ШІ розглядається одночасно як засіб мінімізації ризиків та засіб стимулювання позитивних економічних трансформацій. Існує потреба правового регулювання використання систем ШІ в Україні. Чинна система норм видається недостатньою. Бажано щоб український закон про використання систем ШІ містив положення щодо визначення, яке б чітко обмежило сферу нормативного впливу, структурувало національний юридичний та технічний дискурс, класифікації сфер використання ШІ за небезпекою можливих ризиків, обов'язкової диверсифікації систем ШІ, сфери використання яких характеризуються найбільшим ризиком. Регулювання використання систем ШІ національними правоохоронними має відбуватися у спосіб формулювання спеціальних норм до загальних правил, які названі вище. Відсутність чітких та зрозумілих законодавчих положень про можливі обмеження приватності громадян під час використання технологій ШІ для протидії злочинам, створює реальну небезпеку визнання діяльності правоохоронних органів незаконною навіть за формальною ознакою (не «у відповідності до закону»).

5. Підкреслено, що належний рівень охорони суспільних відносин у сфері формування інформаційного простору, як структурного елемента інформаційної безпеки, видається досяжним за рахунок дотримання ряду ключових положень, серед яких: сприяння довірі та впевненості; захисту приватності та персональних даних; стійкості до кіберзагроз; збереження демократичних цінностей; заохочення інновацій та співпраці; розвитку позитивної цифрової культури; сприяння цифровій інклюзії; підтримки економічного зростання; сприяння міжнародному співробітництву тощо. Реальну та потенційну загрозу для вироблення безпечного та надійного інформаційного простору складають його різноманітні деструктивні прояви, серед яких, зокрема, пропаганда війни, дезінформація та мова ворожнечі,

що можуть мати далекосяжні наслідки як на рівні окремих осіб, суспільств, держав, так і всього міжнародного континууму. Розробка та втілення у життя стратегій боротьби з такими деструктивними проявами інформаційного простору вимагає дотримання справедливого та складного балансу між шкодою, яку вони заподіюють (або можуть заподіяти), та свободою слова як гарантією демократичного розвитку, а також забезпечення комплексного підходу за участі національних урядів, громадянського суспільства, технологічних компаній та розвинутого міжнародного співробітництва.

6. У зв'язку з дослідженням досвіду кримінально-правового регулювання масових розсилок повідомлень електронної пошти у США актуалізовано увагу ще на одній важливій специфіці протидії злочинному використанню інформаційних технологій. Побудова механізмів кримінально-правової охорони має враховувати негативний вплив заборон на соціально корисні відносини. Іншими словами, у випадках коли мінімізація ризиків використання інформаційних технологій можлива шляхом застосування інших, не кримінально-правових інструментів, доцільно використовувати саме їх.

Розділ 2

ПРІОРИТЕТНІ НАПРЯМИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КРИМІНАЛЬНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ

Презентований розділ «Пріоритетні напрями державної політики у сфері кримінально-правового забезпечення інформаційної безпеки» включає в себе такі дослідження: 1) загальні засади державної політики у сфері кримінально-правового забезпечення інформаційної безпеки; 2) інформаційна безпека як складова кримінально-правової політики в умовах воєнного стану; 3) кримінально-правова охорона інформаційного суверенітету; 4) кримінально-правова охорона інформаційної безпеки дітей; 5) караність кримінальних правопорушень проти інформаційної безпеки за кримінальним законодавством України.

Надане дослідження дає змогу читачеві ознайомитися із тим, за допомогою якого інструментарію формується державна політика у сфері кримінально-правового забезпечення інформаційної безпеки. Автори здійснили таке дослідження враховуючи широкомасштабну російську агресію проти України та тривалу деструктивну пропаганду.

Реалізація державної політики у сфері кримінально-правового забезпечення інформаційної безпеки має важливе значення, оскільки її проведення впливає на можливість збереження України як суверенної, незалежної, демократичної та правової держави від час війни. Формування такої політики дає змогу протидіяти як публічним закликам, що притаманні посяганням на національну та громадську безпеку в воєнний час, так і іншим посяганням на інформаційну без-

пеку та кіберпростір. Комплексні правові, економічні, інформаційні та інші заходи протидії можуть надати позитивний ефект, який дозволить мінімізувати та нейтралізувати небезпечний для українського суспільства інформаційний вплив від його.

Від належного здійснення державної політики у сфері кримінально-правового забезпечення інформаційної безпеки залежать перспективи кваліфікації та розслідування кримінальних правопорушень у цій сфері. Наведені питання включають в себе також вирішення проблем кримінально-правового забезпечення свободи думки, совісті і релігії та свободи вираження поглядів, кримінально-правової охорони інформаційного суверенітету, правового регулювання використання ШІ, кримінально-правової охорони інформаційної безпеки дітей, а також караності таких кримінальних правопорушень.

Дослідження інформаційного суверенітету, кримінальних правопорушень, що посягають на інформаційну безпеку та караності цих суспільно небезпечих діянь в поєднанні із вивченням стратегічних та програмних завдань держави в перспективному вимірі дає змогу виявити напрями державної політики у зазначеній сфері та можливості її удосконалення в майбутньому. Очевидно, що на сьогодні домінуючими напрямами в сфері кримінально-правового забезпечення інтересів держави стає охорона національно безпеки, відбиття пропаганди та кібератак держави-агресора, а також приведення нормативно-правових актів до європейських та світових стандартів.

2.1. Загальні засади державної політики у сфері кримінально-правового забезпечення інформаційної безпеки

У Стратегії національної безпеки України зазначено, що «деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність. Відсутність цілісної інформаційної політики держави, слабкість системи стратегічних комунікацій ускладнюють

нейтралізацію цієї загрози» (п. 20)[1]. При цьому «пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції є активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді». Таким чином, деструктивна пропаганда ще до початку широкомасштабної російської агресії визнавалася однією з найбільших загроз для України.

Історично створена в Україні нормативно-правова база в сфері кримінально-правового забезпечення інформаційної безпеки пов'язується із Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. №537-V, Стратегією розвитку інформаційного суспільства в Україні, затвердженою розпорядженням Кабінету Міністрів України від 15.05.2013 р. №386-р (розрахована до 2020 р.), Стратегією цифрової трансформації соціальної сфери, схваленою розпорядженням Кабінету Міністрів України від 28.10.2020 р. №1353-р,, Концепцією розвитку штучного інтелекту в Україні, схваленою розпорядженням Кабінету Міністрів України від 02.12. 2020 р. №1556-р. та ін.

Важливість забезпечення інформаційної безпеки в Україні підтверджується й тим, що ще до початку широкомасштабної війни Указом Президента України №685/2021 було введено в дію рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» (розрахована до 2025 р.). Відповідно до цього державного документу інформаційна безпека України визнається «однією з найважливіших функцій держави». Стратегія була прийнята з метою «посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина»[2].

---

[1] Затверджена Указом Президента України від 14.09.2020 р. №392/2020.

[2] Про Рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки», затв. Указом Президента України

Стратегія інформаційної безпеки надає і визначення інформаційної безпеки України, що наводилось вище у розділі 1.1. цієї монографії. Серед ***глобальних загроз*** Радою Національної безпеки і оборони України були зазначені: 1) збільшення кількості глобальних дезінформаційних кампаній; 2) інформаційна політика російської федерації – загроза не лише для України, але й для інших демократичних держав; 3) соціальні мережі як суб'єкти впливу в інформаційному просторі; 4) недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій. До ***національних викликів та загроз*** віднесено: 1) інформаційний вплив російської федерації як держави-агресора на населення України; 2) інформаційне домінування російської федерації як держави-агресора на тимчасово окупованих територіях України; 3) обмежені можливості реагувати на дезінформаційні кампанії; 4) несформованість системи стратегічних комунікацій; 5) недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів; 6) спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України; 7) доступ до інформації на місцевому рівні; 8) недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам.

Наведені визначення глобальних та національних викликів та загроз для України в сфері інформаційної безпеки та самокритичність щодо їх недоцінки виявилися вкрай своєчасними, оскільки з початком російського широкомасштабного вторгнення саме вони стали більш інтенсивно та агресивно проявлятися в інформаційному, цифровому та кіберпросторі нашої держави. У Стратегії інформаційної безпеки України також було зафіксовано й стратегічні цілі:

«1. *Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної,*

№ 685/2021. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини.

2. *Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності.*

3. *Підвищення рівня медіакультури та медіаграмотності суспільства. Українське суспільство повинне бути захищене від деструктивного впливу дезінформації та маніпулятивної інформації, а медіасередовище – бути соціально відповідальним і функціонувати стабільно*. За таких умов українське суспільство зможе більш ефективно протистояти державі-агресору та залишатися стійким перед широким спектром загроз, зокрема в інформаційній сфері.

4. *Забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів, гарантування їх безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту.*

5. *Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору, а також відновлення їх права на інформацію, що дає їм змогу підтримувати зв'язок з Україною. Одним з основних напрямів внутрішньополітичної діяльності держави є захист прав, свобод і законних інтересів своїх громадян на тимчасово окупованих територіях, реалізація ініціатив щодо реінтеграції цих територій, а також захист прав і свобод корінних народів України*».

Як бачимо, більшість із визначених вище стратегічних цілей пов'язуються із реалізацією державної політики у сфері кримінально-правового забезпечення інформаційної безпеки. Так, наприклад, одним із завдань у межах 5-ої стратегічної цілі, яку поставила перед суспільством Рада Національної безпеки і оборони України, є «інформування громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України, про шкоду, завдану злочинними діями російської федерації, її окупацій-

ної адміністрації на тимчасово окупованій території Автономної Республіки Крим та міста Севастополя, а також контрольованими нею терористичними організаціями на території Донецької та Луганської областей». Таким чином, ще до початку широкомасштабного вторгнення російської федерації до України її дії на тимчасово окупованих територіях, починаючи з 2014 р. були визнані злочинними.

Цікавим є й те, що Стратегія інформаційної безпеки України реалізується також і за допомогою інших програмних документів держави, які якби напряму не стосуються інформаційної безпеки, однак, будучи загалом стратегічними та глобальними цілями для України, опосередковано забезпечують і цей напрям державної політики.

Так, Європейська комісія в своєму звіті по Україні 2023 р. (Брюсель, 08.11.2023, SWD(2023) 699 final) у розділі 7 «Право інтелектуальної власності» констатувала, що «в боротьбі з піратством та контрафактною продукцією залишаються недоліки, оскільки Україна залишається одним із чотирьох основних транзитних пунктів для поставок контрафактної продукції до ЄС»[1]. Тому виглядає не випадковим, що вже наступного дня після оприлюднення звіту Європейської комісії по Україні 09.11.2023 р. Національна рада України з питань телебачення і радіомовлення поповнила Перелік аудіовізуальних медіа-сервісів на замовлення та сервісів провайдерів аудіовізуальних сервісів держави-агресора ще 16-ма сервісами, що не можуть транслюватися в Україні[2]. Важливим є й той факт, що Європейська комісія в різних блоках звіту по Україні 2023 р. розглядає створення електронних сервісів та діджиталізацію, що є продовженням реформ публічного адміністрування, охорони здоров'я, правосуддя та інших

[1] Див.: Ukraine 2023 Report. European Committee. *European Commission:* of. website. URL: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023–11/SWD_2023_699 Ukraine report.pdf

[2] Медіарегулятор вніс 16 медіасервісів до переліку сервісів держави-агресора. 2023. *Національна рада України з питань телебачення і радіомовлення*: оф. вебсайт. URL: https://webportal.nrada.gov.ua/mediaregulyator-vnis-16-mediaservisiv-do-pereliku-servisiv-derzhavy-agresora/

сфер державного життя, як важливу складову протидії корупції та іншим небезпечним викликам[1].

Указом Президента України № 447/2021 було також введено в дію рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію кібербезпеки України». Цією Стратегією були визначені такі загрози кібербезпеці України:

«1) *гібридна агресія Російської Федерації проти України у кіберпросторі*. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності;

2) *кіберзлочинність*, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо;

3) організовані та спонсоровані урядами інших держав *кібератаки, що пов'язані з викраденням у політичних, економічних або військо-*

[1] Див.: Ukraine 2023 Report. European Committee. *European Commission:* of. website. URL: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023–11/SWD_2023_699 Ukraine report.pdf

вих цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності. Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію;

4) *використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності»*.

Для формування потенціалу стримування кіберзлочинності Стратегія визначила необхідним створення *стратегічної цілі ефективної їй протидії,* якою «Україна забезпечить набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів». Важливим є й те, що Стратегія передбачила, яким шляхом має бути досягнута така стратегічна ціль:

«а) завершення імплементації в законодавство України положень Конвенції про кіберзлочинність;

б) врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав – членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки;

в) розроблення концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей);

г) запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

д) розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних вебсайтах;

е) розроблення методики проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечення проведення таких досліджень;

є) розроблення методики комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створення необхідних умов для її практичної реалізації;

ж) запровадження механізмів ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України;

з) врегулювання на законодавчому рівні правового статусу криптовалют;

и) проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози;

і) забезпечення підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів;

ї) забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів;

к) залучення приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів».

Треба підкреслити, що державна політика у сфері кримінально-правового забезпечення інформаційної безпеки реалізується різними нормативно-правовими актами. Однак, як вже було зазначено, певні з них формують напрями такої кримінально-правової політики тільки опосередковано. Так, у Концепції розвитку штучного інтелекту в Україні передбачається, що «застосування технологій штучного інтелекту в забезпеченні інформаційної безпеки є одним із факторів,

що сприятиме забезпеченню національних інтересів. Зокрема, моніторинг соціальних мереж та інтернет-ресурсів електронних медіа з використанням технологій штучного інтелекту дає можливість виявляти системні тренди і проблематику, діяти на випередження, аналізувати цільову аудиторію». Зазначено, що для досягнення мети Концепції у зазначеній сфері варто забезпечити виконання певних завдань, зокрема, «*виявлення, запобігання і нейтралізація реальних і потенційних загроз поширення засобами масової інформації культу насильства, жорстокості, порнографії, намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації*».

КК України є найбільш вагомим охоронним нормативно-правовим актом, що дозволяє здійснювати захист суспільних відносин в окремих сферах, власними засобами впливати на їх регулювання та формувати державну політику, у т. ч. у сфері забезпечення інформаційної безпеки.

Прийнято вважати, що ядром такої кримінально-правової охорони є розділ XVI Особливої частини КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Цей розділ включає такі кримінальні правопорушення: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України); 2) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1 КК України); 3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2 КК України); 4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України); 5) порушення правил експлуатації елек-

тронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України); 6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363[1] КК України).

Разом із цим у період широкомасштабної російської воєнної агресії проти України державна політика у сфері кримінально-правового забезпечення інформаційної безпеки в Україні не може бути сконцентрована лише на протидії кримінальним правопорушенням, визначеним у розділі XVI Особливої частини КК. Як демонструють сформовані вище стратегії та концепції, наявне розуміння того, що основні небезпеки інформаційній безпеці йдуть з боку держави-агресора і спрямовані на руйнацію суверенітету, незалежності та самих основ конституційного ладу України, а, отже, важливим стає відображення в нормах КК саме цього напряму забезпечення інформаційної безпеки. З іншого боку, наявним є і процес зовнішнього впливу, який спрямований на європейську та євроатлантичну інтеграцію, що вимагає проведення багатьох реформ, їх фінансування, корегування, звітування, тощо. Це означає, що державна політика у сфері кримінально-правового забезпечення інформаційної безпеки в Україні повинна бути спрямована не тільки на відображені в нормах КК руйнівних для українського суспільства наслідків російської агресії, але й на своєчасному урахуванні європейських та євроатлантичних стандартів та правил, спрямованих на охорону сфери інформаційної безпеки, що здійснити під час війни хоча і складно, однак, є необхідним для збереження держави. Робота в останньому напрямі потребує виважених порівняльних досліджень та пошагової імплементації.

Саме тому на початку широкомасштабного російсько-українського воєнного протистояння законодавець України, треба надати йому належне, доволі оперативно доповнив КК України важливими нормативами, реалізувавши тим актуальні для сьогодення потреби держави у забезпеченні інформаційної безпеки. Прикладом є зміни та доповнення, що були внесені до Особливої частини КК пісс-

ля 24.02.2022 р. Так, важливими, можливо, і ключовими в контексті забезпечення інформаційної безпеки в Україні, стали нормативні положення, спрямовані на потужну протидію ворожим публічним закликам (ч. 2 ст. 109, ч. 1 ст. 110, ч.ч. 1, 5 ст. 111^1, ч. 1 ст. 258^2, ч. 1 ст. 295, ч. 1 ст. 299, ч. 2 ст. 442 КК України) і особливо – небезпечній для українського суспільства пропаганді (ч. 3 ст. 111^1, ст. 299, ст. 436, ст. 436^1 КК України).

Необхідну роль у формуванні державної політики у сфері кримінально-правового забезпечення інформаційної безпеки відіграє ЄКПЛ та практика Європейського суду з прав людини (далі – ЄСПЛ), що на законодавчому рівні визнані в Україні джерелом права. Помітними в цьому плані є ст. 9 та ст. 10 Конвенції, якими визначені та здійснюється захист «Свободи думки, совісті і релігії» та «Свободи вираження поглядів». При цьому важливим є не тільки факт закріплення в Конвенції зазначених свобод, але й передбачення цим міжнародним актом певних обмежень, необхідних для підтримання соціальної пропорційності.

Так, за ст. 9 Конвенції «свобода сповідувати свою релігію або переконання підлягає лише таким обмеженням, що встановлені законом і є необхідними в демократичному суспільстві в інтересах громадської безпеки, для охорони публічного порядку, здоров'я чи моралі або для захисту прав і свобод інших осіб». Довідник із застосування цієї статті, вказує, що «водночас стаття 18 Міжнародного пакту про громадянські та політичні права in fine уточнює, що держави, які беруть участь у цьому Пакті, зобов'язуються поважати свободу батьків і у відповідних випадках законних опікунів забезпечувати релігійне і моральне виховання своїх дітей відповідно до своїх власних переконань. Стаття 26 Пакту проголошує загальний принцип заборони дискримінації, зокрема за ознакою релігії». Також варто закцентувати увагу й на тому, що ЄСПЛ «дійшов висновку про відсутність порушення ст. 9 у справі, де заявники-організації, зайняті поширенням вчення Бхаган Шрі Раджніша (Ошо), скаржились на неодноразове вживання для його визначення у деяких офіційних повідомленнях німецького федерального уряду і його членів термінів «секта», «молодіжна секта», «психо-секта», «псевдорелігія», «деструк-

тивний релігійний рух», «рух, що маніпулює своїми членами» тощо… Відштовхуючись від припущення, що мало місце втручання у реалізацію прав, гарантованих ст. 9, ЄСПЛ постановив, що це втручання переслідувало законні цілі (громадська безпека, захист порядку та прав і свобод інших осіб) і було пропорційне відносно цих цілей (Leela Förderkreis e.V. і Інші проти Німеччини)»[1].

За ст. 10 Конвенції «здійснення цих свобод *(мається на увазі – свобод дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів)*, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду».

При розгляді обмежень прав на свободу зібрань та об'єднань дослідники практики ЄСПЛ зазначають, що таке право не є абсолютним: «воно може бути обмежене, відповідно до п. 2 ст. 11 Конвенції. Втручання у здійснення цього права не вимагає безпосередньої абсолютної юридичної або фактичної заборони, але може складатися з інших різних заходів, які вживаються органами влади (Кудревічюс та інші проти Литви (Kudrevicius and Others v. Lithuania) [ВП], § 100)»[2]. Водночас в Україні на сьогодні така заборона наявна. Так, у п. 8 ч. 1 ст. 8 Закону України «Про правовий режим воєнного стану» окремо передбачено, що в Україні або в окремих її місцевостях, де введено воєнний стан, військове командування разом із військовими адміністраціями (у разі їх утворення) можуть самостійно або із залученням органів

[1] Див.: Довідник із застосування статті 9 Конвенції. *European Court of Human Rights*: of. website. URL: https://www.echr.coe.int/documents/d/echr/Guide_Art_9_UKR

[2] Див.: Посібник за статтею 11 Конвенції про захист прав людини та основоположних свобод. *European Court of Human Rights*: of. website. URL: https://unba.org.ua/assets/uploads/75f3bb7ffb475097735f_file.pdf; Guide on Article 11 of the European Convention on Human Rights. *European Court of Human Rights*: of. website. URL: https://www.echr.coe.int/Documents/Guide_Art_11_ENG.pdf

виконавчої влади, Ради міністрів Автономної Республіки Крим, органів місцевого самоврядування запроваджувати та здійснювати в межах тимчасових обмежень конституційних прав і свобод людини і громадянина, а також прав і законних інтересів юридичних осіб, передбачених указом Президента України про введення воєнного стану, такі заходи правового режиму воєнного стану – забороняти проведення мирних зборів, мітингів, походів і демонстрацій, інших масових заходів.

Здійснення ворожих публічних закликів у їх крайніх проявах пов'язується із посяганням на національну, громадську безпеку або безпеку миру, безпеку людства та міжнародного правопорядку (захист яких забезпечують норми розділів I, IX, XX Особливої частини КК України). Найбільш інтенсивним інформаційним впливом на усвідомлене сприйняття інформації є здійснення вкрай небезпечної для українського суспільства пропаганди.

КК України в різних розділах Особливої частини передбачає відповідальність за здійснення пропаганди в певних для такої протиправної діяльності формах. Форми пропаганди проявляються через: 1) колабораційну діяльність – ч. 3 ст. 111^1 КК України; 2) ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію – ст. 300 КК України; 3) пропаганду війни – ст. 436 КК України; 4) пропаганду комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів – ст. 436^1 КК України. Визначення, що таке «пропаганда» кримінальне законодавство не надає, хоча така поведінка, як суспільно небезпечне діяння, що передбачене КК, має достатньо широкі вектори соціальної руйнації. Зокрема, спричиняє або може спричинити шкоду: основам національної безпеки; громадській безпеці; громадському порядку; миру, безпеці людства та міжнародному правопорядку й іншим, не менш важливим для суспільного життя відносинам.

Не менш важливим чинником забезпечення послідовної державної політики у сфері боротьби зі злочинністю, у тому числі й у сфері інформаційної безпеки, є показник стабільності кримінального законодавства. Стабільність більшості його норм віддзеркалює віднос-

ну незмінність нормативного забезпечення боротьби зі злочинністю, а також наступність тих концептуальних положень, які в них були закладені, що довели на правозастосовному рівні свою ефективність. До числа таких норм можна віднести положення ст. 300 КК України «Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію» та ст. 436 КК «Пропаганда війни». Більш ніж 20-річний час їх реалізації дозволив виробити відносно однозначне розуміння їх змісту і, що головне, більш-менш однакову практику їх застосування.

В останні роки кримінальне законодавство України поповнилося значною кількістю нових норм, необхідність прийняття яких була обумовлена рядом обставин, у тому числі політичного характеру. Останніми, по-перше, є послідовне нарощування євроінтеграційного вектору розвитку України; по-друге, кардинальні зміни ідеологічних поглядів більшої частини населення на сутність комуністичного та націонал-соціалістичного (нацистського) режимів державного устрою; по-третє, це воєнний стан, в якому перебуває суспільство внаслідок російської агресії проти України. Вплив зазначених обставин є вирішальним у розумінні змісту законодавчих новел, як регулятивного, так і охоронного характеру. До числа останніх варто віднести й норми КК, якими встановлена відповідальність за вчинення суспільно небезпечних діянь, пов'язаних із пропагандою, шкідливою для сучасного стану українського суспільства. Безпосередній зв'язок з положеннями регуляторного характеру має, зокрема, ст. 436^1 КК України – «Виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів». У диспозиції ч. 1 цієї статті прямо вказано на Закон України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки» від 09.04.2015 р. №317-VIII. Звернення до цього Закону дає можливість достатнього розуміння як змісту, так і призначення норми ст. 436^1 КК України. Саме у ст. 2 цього Закону надається визначення пропаганди комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів як «пу-

блічного заперечення, зокрема через медіа, злочинного характеру комуністичного тоталітарного режиму 1917–1991 років в Україні, націонал-соціалістичного (нацистського) тоталітарного режиму, поширення інформації, спрямованої на виправдання злочинного характеру комуністичного, націонал-соціалістичного (нацистського) тоталітарних режимів, діяльності радянських органів державної безпеки, встановлення радянської влади на території України або в окремих адміністративно-територіальних одиницях, переслідування учасників боротьби за незалежність України у XX столітті, виготовлення та/або поширення, а також публічне використання продукції, що містить символіку комуністичного, націонал-соціалістичного (нацистського) тоталітарних режимів».

З початком російської агресії проти України Законом України «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колаборaційну діяльність» від 03.03.2022 р. № 2108-IX було криміналізовано колаборaційну діяльність та передбачено відповідальність за «здійснення громадянином України пропаганди у закладах освіти незалежно від типів та форм власності з метою сприяння здійсненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України, а також дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти» (ст. 111[1] КК України).

Не можна відкидати очевидний зв'язок пропаганди та воєнних злочинів. Так, у довідковому виданні «Міжнародне гуманітарне право. Загальний курс» Н. Мельцера, виданого під егідою Міжнародного Червоного Хреста, наголошується, що держава, яка окуповує, не може використовувати пропаганду, спрямовану на добровільний вступ до окупаційних сил[1]. Також у ст. 51 Конвенції про захист цивільного населення під час війни вказується, що «окупаційна держава не має права примушувати осіб, що перебувають під захистом, служити в її збройних чи допоміжних силах».

[1] Мельцер Н. Международное гуманитарное право. Общая часть. МККК. С. 287.

У І додатковому протоколі до Женевських конвенцій зазначається, що сторони, які перебувають у конфлікті, вживають усіх практично можливих заходів для того, щоб діти, які не досягли п'ятнадцятирічного віку, не брали безпосередньої участі у воєнних діях, і, зокрема, сторони утримуються від вербування їх у свої збройні сили. При вербуванні із числа осіб, які досягли п'ятнадцятирічного віку, але яким ще не виповнилося вісімнадцяти років, сторони, що перебувають у конфлікті, прагнуть віддавати перевагу особам старшого віку. А вже в ІІ додатковому протоколі до Женевських конвенцій також вказується, що «діти, які не досягли п'ятнадцятирічного віку, не підлягають вербуванню у збройні сили або групи, і їм не дозволяється брати участь у воєнних діях», але в цьому разі нічого не зазначається про заборону пропаганди. Серед звичаїв ведення війни також відзначається, що «діти не повинні вербуватися у збройні сили або збройні угруповування» (норма 136)[1].

Таким чином, можна зробити висновок, що пропаганда війни є близьким кримінальним правопорушенням до воєнних злочинів, але ним прямо не визнається. Тільки у випадку набуття ознак примушування або вербування можна ставити питання про вчинення воєнного злочину, що порушує закони та звичаї війни (ст. 438 КК України). На практиці, на жаль, трапляються випадки вільного трактування примушування як пропаганди, що призводить до притягнення до кримінальної відповідальності за пропаганду служби в армії як воєнного злочину – «Порушення законів та звичаїв війни» (ст. 438 КК України). Так, Подільським районним судом м. Києва була засуджена особа за пропаганду служби в армії окупуючої держави-Російської Федерації. Суд, посилаючись, на ст. 51 Конвенції про захист цивільного населення під час війни інтерпретував окремі заяви в ЗМІ та іншу діяльність підсудного в м. Севастополь та АР Крим як здійснення пропаганди та порушення законів ведення війни[2]. Даний при-

[1] Хенкернс Ж.-М., Досвальд-Бек Л. Обычное международное гуманитарное право. Нормы.МККК, 2006. С. 617.

[2] Вирок Подільського районного суду м. Києва від 15.06.2023 р. (справа №758/16427/21; провадження № 1-кп/758/422/23). Єдиний державний реєстр судових рішень: оф. вебсайт. URL: https://reyestr.court.gov.ua/Review/111764865

клад демонструє необхідність проведення розмежування між воєнними та іншими злочинами проти миру, безпеки людства та міжнародного правопорядку, а також розмежування термінів «пропаганда», «примушування» та «вербування». На нашу думку, суд не може їх вільно використовувати та розглядати їх такі, що мають однаковий зміст.

Варто звернути увагу на особливу суспільну небезпечність і геноциду у формі публічних закликів до геноциду, а також виготовлення матеріалів із закликами до геноциду з метою їх розповсюдження або розповсюдження таких матеріалів» (ч. 2 ст. 442 КК України). Геноцид є одним із злочинів, що порушує норми міжнародного права і саме через його винятковість була прийнята Конвенція ООН про запобігання злочину геноциду і покарання за нього 1948 р. У ст. III цієї Конвенції також передбачено кримінальну відповідальність за «пряме і публічне підбурювання до здійснення геноциду», що фактично і імплементовано в ч. 2 ст. 442 КК України. Особливістю суб'єкта, відповідального за вчинення даного діяння є те, що «особи, що чинять геноцид чи які-небудь інші з перерахованих у статті III діянь, підлягають покаранню, незалежно від того, чи є вони відповідальними по конституції правителями, посадовими чи приватними особами», а також «у відношенні видачі винних геноцид і інші перераховані в статті III діяння не розглядаються як політичні злочини» (ст.ст. IV, VII Конвенції).

У цілому реалізація державної політики у сфері кримінально-правового забезпечення інформаційної безпеки має важливе кримінально-правове значення, оскільки впливає на збереження України як суверенної, незалежної, демократичної та правової держави. Формування окремого напряму державної політики у сфері кримінально-правового забезпечення інформаційної безпеки надасть можливість поступової спланованої протидії як публічним закликам, що притаманні посяганням на національну та громадську безпеку, так і ефективній протидії пропаганді та воєнній агресії в цілому. Правові, економічні, інформаційні та інші заходи протидії здатні надати позитивний ефект, що дозволить мінімізувати та нейтралізувати небезпечний інформаційний вплив на українське суспільство.

2.2. Інформаційна безпека як складова кримінально-правової політики в умовах воєнного стану

Під кримінально-правовою політикою в теорії кримінального права зазвичай розуміють основний системоутворюючий елемент політики держави у сфері боротьби зі злочинністю[1]. По суті це державна політика з протидії злочинності, що проявляється у визначенні концептуальних, правових, організаційних і навіть ресурсних заходів, направлених на боротьбу зі злочинністю, усунення її причин та мінімізацію наслідків за рахунок зусиль громадянського суспільства та відповідної діяльності державних органів[2]. Кримінально-правова політика пройшла досить складний час від невизнання її існування до визнання необхідності її дослідження і врахування при вдосконаленні законодавства і практики його застосування.

Однак кримінально-правова політика є змінним явищем, яке реагує на правову політику держави в цілому. Так, 28 грудня 2021 р. указом Президента України № 685/2021 була затверджена Стратегія інформаційної безпеки, аналіз положень якої надавався вище[3]. Розпочата росією 24 лютого 2022 р. війна проти України внесла свої корективи у формування кримінально-правової політики нашої держави. Тому ще більшої актуальності набуло питання забезпечення інформаційної безпеки держави, тобто вжиття дієвих заходів вповноважених державних органів в інформаційній сфері, спрямованих на захист національної безпеки та оборони України. У зв'язку із цим Президент України підписав Указ № 152/2022, яким було введено в дію Рішення Ради національної безпеки і оборони Укра-

---

[1] Борисов В. І., Фріс П. Л. Засади сучасної кримінально-правової політики України. *Питання боротьби зі злочинністю.* 2014. Вип. 27. С. 32.

[2] Остроглядо О. Поняття та ознаки кримінально-правової політики. *Jurnalul juridic national: teorie şi practică.* August 2020. С. 96.

[3] Стратегія інформаційної безпеки : затв. указом Президента України від 28 груд. 2021 р. № 685/2021. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

їни «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»[1].

З моменту підписання Президентом України указу «Про введення воєнного стану в Україні» від 24.02.2022 р. №64/2022[2] були внесені зміни до багатьох нормативно-правових актів з метою урахування сучасних реалій. Зміни зокрема торкнулися врегулювання окремих аспектів щодо технічного фіксування інформації; врегулювання питання інформаційних правовідносин щодо заборони поширювати деяку інформацію, зважаючи на суспільну небезпечність такого поширення; встановлення та посилення відповідальності за поширення конкретних видів інформації; врегулювання процесуальних моментів, пов'язаних з вилученням інформації. Оновлена система заходів кримінально-правової політики запобігання злочинним посяганням на основи національної безпеки мала відповідати реаліям сьогодення та бути здатною нейтралізувати такі посягання не лише зараз, а й в майбутньому.

Проблема убезпечення інформації не є новою, але була й залишається вкрай актуальною, особливо тепер, у часи воєнного стану, оголошеного у зв'язку з воєнною агресією з боку росії проти України. Забезпечення інформаційної безпеки здійснюється на основі поєднання правових, адміністративних, організаційних, технічних та інших форм діяльності органів державної влади у взаємодії з органами місцевого самоврядування, підприємствами, установами, організаціями, громадянами та їх об'єднаннями.

У системі правового регулювання убезпечення інформації помітне місце займають норми, спрямовані на охорону інформаційної безпеки від кримінально-протиправних посягань. Формулюючи диспозиції норм Особливої частини КК, законодавець уводить до них найбільш характерні (істотні) ознаки, і, як правило, такі, що є типо-

[1] Щодо реалізації єдиної інформаційної політики в умовах воєнного стану : рішення Ради національної безпеки і оборони України, введене в дію указом Президента України від 19 берез. 2022 р. №152/2022. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text.

[2] Про введення воєнного стану в Україні : указ Президента України від 24 лют. 2022 р. №64/2022. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text.

вими для явищ, які для суспільства є небезпечними. Зазвичай такі ознаки іменують конститутивними. Для кримінального правопорушення та визначення його складу такі ознаки є обов'язковими. Це стосується й терміна «інформація», яку законодавець використовує як певну ознаку кримінального правопорушення, визначаючи її у відповідній нормі. Водночас смислове навантаження на цей термін достатньо різне. Будучи уведеним до норми КК законодавцем як ознака кримінального правопорушення, термін «інформація» може визначати засіб його вчинення, знаряддя або предмет[1] кримінального правопорушення, що залежить від особливостей прояву правопорушення в об'єктивній дійсності. Далі, завдяки предмету можна отримати більш точне уявлення й про об'єкт кримінально-правової охорони.

В умовах здійснення російської збройної агресії проти України питання протидії поширенню різноманітної небезпечної для держави інформації набуло особливої актуальності, що законодавцем, треба надати належне, було враховано доволі оперативно[2].

Так, Законом України «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність» від 03.03.2022 р. №2108-IX КК України був доповнений ст. 111^1 «Колабораційна діяльність»[3], яка містить значну кількість складів кримінальних правопорушень щодо співпраці з державою-агресором. За своєю суттю це різні склади кримінальних правопорушень, проте деякі з них, конкурують не лише між собою, а й з існуючими раніше складами. Це викликало чимало дис-

---

[1] Музика А. А., Лащук Є. В. Предмет злочину: теоретичні основи пізнання: монографія. К.: ПАЛИВОДА А. В., 2011. С. 127.

[2] Борисов В. І., Байда А. О., Базелюк В. В. Інформаційна безпека як споріднена ознака кримінальних правопорушень, передбачених ст.ст. 114^2 та 436^2 КК України: питання розмежування. *Сучасний розвиток державотворення та правотворення в Україні: проблеми теорії та практики*: матеріали X міжнародної науково-практичної конференції онлайн (м. Маріуполь, 23 червня 2022 р.). Зб. тез наук. праць / за заг. редакцією М. В. Трофименко. Київ: МДУ, 2022. С. 34. URL: http://mdu.in.ua/Nauch/Konf/2022/zbirnik_materialiv_konferenciji_23.06.2022.pdf.

[3] Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність : Закон України від 3 берез. 2022 р. №2108-IX. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2108–20#n12.

кусій як серед науковців, так і практиків. Зокрема, до ст. 111 «Державна зрада» з метою розширення підстав її застосування вносилися деякі зміни, тому наразі іноді виникають складнощі у розмежуванні зазначених складів кримінальних правопорушень. Проте однією з основних відмінностей є те, що колабораційні дії вчиняються суб'єктом вже в умовах агресії або окупації. Також варто враховувати, що суб'єктом державної зради може бути лише громадянин України, а за ч. 4 та ч. 6 ст. 111[1] КК – у тому числі й іноземці та особи без громадянства[1]. Особливо гостро стоїть питання відмежування державної зради від кримінального правопорушення, передбаченого ч. 7 ст. 111[1] КК (добровільне зайняття громадянином України посади в незаконних судових або правоохоронних органах, створених на тимчасово окупованій території, а також добровільна участь громадянина України в незаконних збройних чи воєнізованих формуваннях, створених на тимчасово окупованій території, та/або в збройних формуваннях держави-агресора чи надання таким формуванням допомоги у веденні бойових дій проти Збройних Сил України та інших військових формувань, утворених відповідно до законів України, добровольчих формувань, що були утворені або самоорганізовувалися для захисту незалежності, суверенітету та територіальної цілісності України). До появи цієї норми подібні дії можна було кваліфікувати як державну зраду у формі надання іноземній державі допомоги у проведенні підривної діяльності проти України або переходу на бік ворога в період збройного конфлікту. Більшість науковців наполягають на тому, що колабораційна діяльність є спеціальним видом державної зради. Хоча і не зовсім зрозуміло, чим керувався законодавець пом'якшуючи відповідальність за такі дії, як участь у збройних формуваннях держави-агресора, які традиційно вважалися державною зрадою. Проте між цими складами злочинів є й певні відмінності. Зайняття грома-

[1] Музика А. А. Норми про кримінальну відповідальність за колабораційну діяльність потребують актуальних поправок. Кримінально-правові відповіді на виклики воєнного стану в Україні: матеріали міжнар. наук. конф., м. Харків, 5 трав. 2022 р. / упоряд. та заг. ред.: Ю. В. Баулін, Ю. А. Пономаренко; Нац. юрид. ун-т ім. Ярослава Мудрого; Нац. шк. суддів України; Громад. орг. «Всеукр. асоц. кримін. права»; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків: Право, 2022. С. 103 – 116.

дянином України посади в незаконних судових або правоохоронних органах та добровільна участь громадянина України в незаконних збройних чи воєнізованих формуваннях як форма колабораційної діяльності мають місце лише в органах, створених на тимчасово окупованій території. Тобто головною відмінністю тут виступає місце вчинення зрадницьких дій. Щодо участі у збройних формуваннях держави-агресора чи надання таким формуванням допомоги у веденні бойових дій проти Збройних сил України та інших військових формувань, утворених відповідно до законів України, добровольчих формувань, що були утворені або самоорганізовувалися для захисту незалежності, суверенітету та територіальної цілісності України, то тут відсутня вказівка законодавця на місце вчинення такого діяння. Немає у ч. 7 ст. 111[1] КК, на відміну від ч. 6 цієї норми, і застереження законодавця на «відсутність ознак державної зради». У ч. 2 ст. 111 КК обов'язковою ознакою об'єктивної сторони є час вчинення діяння (в умовах воєнного стану). Із зазначеного випливає, що ст. 111 КК та ч. 7 ст. 111[1] КК мають деякі відмінності, проте у більшості випадків діяння будуть підпадати під обидві норми, що співвідносяться як загальна та спеціальна (привілейована) норма відповідно[1]. Тобто по суті колабораційна діяльність є спеціальним видом державної зради, тому, якщо при кваліфікації виникають сумніви, то перевага повинна надаватися спеціальній нормі.

Законом України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» від 03.03.2022 р. № 2110-IX КК України був доповнений ст. 436[2] КК «Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників»[2].

---

[1] Збірник пропозицій та роз'яснень з актуальних питань права в умовах війни фахівців сектору дослідження кримінально-правових проблем боротьби зі злочинністю Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України / упоряд.: Л. М. Демидова, М. В. Шепітько, Н. В. Шульженко та ін. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2022. С. 25.

[2] Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої

Однак, як видається, ця норма конкурує з положеннями ч. 1 ст. 111[1] КК, що передбачає відповідальність за публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики громадянином України до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України. Розмежувати зазначені склади можна передусім за змістом заперечення: у ч. 1 ст. 111[1] КК мова йде про заперечення будь-якої агресії, а у ст. 436[2] КК – агресії рф проти України, розпочатої у 2014 р. Різними ці норми є і за характером (способом) заперечення: у ч. 1 ст. 111[1] КК передбачене тільки публічне заперечення, а у ст. 436[2] КК – як публічне, так і непублічне. Відповідно до Примітки до ст. 111[1] КК публічним вважається поширення закликів або висловлення заперечення до невизначеного кола осіб, зокрема у мережі Інтернет або за допомогою засобів масової інформації. Відрізняються досліджувані норми і за суб'єктом кримінального правопорушення: у ч. 1 ст. 111[1] КК суб'єктом є лише громадянин України, а у ст. 436[2] КК України суб'єкт загальний, тобто громадянин України, іноземець та особа без громадянства[1].

Законом України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» від 24.03.2022 р.

інформаційної продукції: Закон України від 3 берез. 2022 р. №2110-IX. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2110–20#n20.

[1] Використано матеріали науково-практичного вебінару «Державна зрада і суміжні злочини проти основ національної безпеки України: питання кваліфікації, розмежування і відповідальність», доповідь Рубащенко М. А. Вебінар відбувся 2 червня 2022 р. URL: https://www.youtube.com/watch?v=pscrcWAa9bk ; https://www.youtube.com/watch?v=IPFcA4-YpC0…

№ 2160-IX КК України був доповнений ст. 114[2] «Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану»[1]. Особливістю цієї норми є те, що перелічені в ній діяння є кримінально-караними лише у випадку, коли вони вчиняються в умовах воєнного або надзвичайного стану. Хоча проблем з відмежуванням цієї норми від інших на практиці не виникає, проте ст. 114[2] КК має свої недоліки. Як зауважив Р. О. Мовчан, недоцільною видається паралельна вказівка у відповідному переліку на «зброю» та «озброєння», які по суті є синонімами. Однак, навіть одночасне згадування про «зброю» та «озброєння» (як і вказівка на бойові припаси) не дозволяє охопити всі ті предмети, одні з яких вже надаються нашій державі, а надання інших можливе (принаймні на це хочеться сподіватися) у перспективі. Відповідно до розділу І Зводу відомостей, що становлять державну таємницю «озброєнням» необхідно вважати – озброєння стрілецьке та артилерійське, системи (комплекси) ракетні і ракетно-космічні, керовані (некеровані) ракети та їх складові частини, комплекси (установки) для їх запуску та складові одиниці до них, засоби керування зброєю (вогнем), системи дистанційного керування ракетами, обладнання для транспортування і обслуговування ракет, апарати торпедні та бомбомети для глибинних бомб[2]. Із офіційних джерел відомо, що деякі із цих складових (стрілецьке озброєння, керовані ракети тощо) вже були отримані Україною. Водночас на сучасному етапі війни з рф наша держава не менше, а на-

[1] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24 березня 2022 р. № 2160-IX. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2160–20#n10.

[2] Звід відомостей, що становлять державну таємницю, затв. наказом Центрального управління Служби безпеки України 23 груд. 2020 р. № 383. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text.

певно навіть більше потребує і тому наразі найчастіше звертається до іноземних партнерів із закликами про виділення літаків, гелікоптерів, безпілотників, танків, бойових машин, бронетранспортерів, технічних засобів захисту апаратури, апаратури для розвідки тощо. Очевидно, що поширення інформації про переміщення згаданих товарів, зокрема і територією України, є вкрай небажаним, а з точки зору кримінального права – просто надзвичайно суспільно небезпечним, адже може призвести до відповідної реакції ворога на постачання цієї техніки, що може істотно вплинути на перебіг війни. І ось тут виникає головна проблема – ні танки, ні бронемашини, ні бронетранспортери, ні гелікоптери, ні жоден з інших названих вище товарів, які Україна вже отримала або лише бажає отримати (літаки, безпілотники, технічні засоби захисту апаратури, апаратура для розвідки тощо), не охоплюються вказаним у ст. 114^2 КК поняттям «озброєння», адже не входять до жодної із тих складових, що перераховані у відповідному наведеному вище нормативному визначенні. А це означає, що несанкціоноване поширення відповідної інформації про ці предмети не може кваліфікуватися за ст. 114^2 КК[1].

Законом України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки» від 14.04.2022 р. № 2198-IX КК України був доповнений ст. 111^2 КК «Пособництво державі-агресору»[2]. Однією із альтернативних форм цього кримінального правопорушення є добровільний збір, підготовка та/або передача матеріальних ресурсів або інших активів представникам держави-

[1] Мовчан Р. О. Аналіз кримінально-правової новели про несанкціоноване поширення військово значущої інформації (ст. 114–2 Кримінального кодексу України). *Юридичний науковий електронний журнал.* 2022. № 4. С. 328. URL: http://lsej.org.ua/4_2022/77.pdf.

[2] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки : Закон України від 14 квіт. 2022 р. № 2198-IX. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2198–20#n8.

агресора, її збройним формуванням та/або окупаційній адміністрації держави-агресора. Фактично зазначене положення дублює ч. 4 ст. 111[1] КК, яка передбачає відповідальність за передачу матеріальних ресурсів незаконним збройним чи воєнізованим формуванням, створеним на тимчасово окупованій території, та/або збройним чи воєнізованим формуванням держави-агресора, та/або провадження господарської діяльності у взаємодії з державою-агресором, незаконними органами влади, створеними на тимчасово окупованій території, у тому числі окупаційною адміністрацією держави-агресора. Така ситуація є законодавчою помилкою, яка потребує негайного вирішення, особливо зважаючи на суттєво відмінні санкції зазначених кримінальних правопорушень (ч. 4 ст. 111[1] КК карається штрафом до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до п'яти років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від десяти до п'ятнадцяти років та з конфіскацією майна, а ст. 111[2] КК – позбавленням волі на строк від десяти до дванадцяти років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від десяти до п'ятнадцяти років та з конфіскацією майна або без такої). Наразі ж за загальним правилом кваліфікація кримінального правопорушення за наявності конкуренції кримінально-правових норм, одна з яких передбачає склад кримінального правопорушення з привілейованими ознаками, повинна здійснюватися за привілейованою нормою, тобто тією, яка містить менш тяжке кримінальне правопорушення[1], хоча є й інші точки зору. Так, М. І. Хавронюк вважає, що при розв'язанні цієї колізії варто відштовхуватися від правил подолання темпоральних колізій, враховуючи що застосуванню підлягає більш новий закон. Учений небезпідставно таку ситуацію відніс до одного з різновидів «порушень принципу пропорційності». Він, зокрема, вбачає прояв помилки в тому, що, ігноруючи факт наявності в КК статті, яка вже передбачає кримінальну відповідальність за певне діяння, законодавець знову криміналізував його, застосувавши ті самі або схожі формулювання і не виокреомивши ознаки,

[1] Кримінальне право (Особлива частина): підручник / за ред. О. О. Дудорова, Є. О. Письменського. Т. 1. Луганськ: видавництво «Елтон-2». 2012. С. 45.

що дали б змогу чітко розмежувати відповідні кримінальні правопорушення, зокрема за правилами конкуренції статей про спеціальний і загальний склади правопорушення[1]. Водночас М. І. Хавронюк пропонує скасувати окремі положення ст. 111[2] КК, так як вони значною мірою дублюють ст. 111[1] КК[2].

Таким чином, формування інформаційної безпеки в умовах військової агресії є комплексом політичної, правової і технічної діяльності уповноважених органів, що спрямована на захист громадян, суспільства та держави. Розвиток нормативно-правових засад управління національною безпекою проводиться шляхом розробки відповідних законів, тому кримінальне законодавство нашої держави останнім часом зазнало суттєвих змін. Безумовно такі доповнення є позитивними та були обумовлені суспільною необхідністю. Однак закон про кримінальну відповідальність у цій частині ще потребує змін та доопрацювань, оскільки доповнення вносилися в складних умовах та у стислі строки.

2.3. Кримінально-правова охорона інформаційного суверенітету

Зміна парадигми суспільного життя, викликана процесами всеохоплюючої інформатизації та формуванням глобального інформаційного простору, поставила необхідність чергового переосмислення змісту та дієвості концепції суверенітету держави відповідно до сучасних умов. Зазначені процеси у поєднанні з відчутним деструктивним впливом у вигляді глобальних інформаційних загроз здатні впливати на потенціал суверенної спроможності держави проводити самостійну та незалежну як внутрішню, так і зовнішню інформаційну політику. Основна мета цих політик полягає у забезпеченні опти-

[1] Використані матеріали: Хавронюк Микола. Помилки у законах воєнного часу щодо змін Кримінального кодексу України. *Facebook*: вебсайт. URL: https://www.facebook.com/nikolaj. havronuk.

[2] Колабораціонізм чи державна зрада: коментар Миколи Хавронюка. 2022. *Центр політико-правових реформ*: вебсайт. URL: https://pravo.org.ua/blogs/kolaboratsionizm-chy-derzhavna-zrada-komentar-mykoly-havronyuka/.

мального регулювання суспільних відносин, що виникають з приводу формування, використання й захисту доступних інформаційних ресурсів, гарантування їх безпечності, виходячи з національних інтересів держави, а також задоволення інших потреб та інтересів користувачів, які перебувають під юрисдикцією конкретної держави, у поєднанні із реалізацією принципу рівноправного та незалежного міжнародного співробітництва у цій сфері.

Враховуючи зазначені чинники, помітним стало існування активного наукового дискурсу, здебільшого, у царині філософії, політології, загальної теорії права, конституційного та адміністративного права щодо існування інформаційного суверенітету як складової державного суверенітету. Однак, не стала виключенням й наука кримінального права. Суттєвими здобутками, що заклали підвалини до дослідження проблем інформаційного суверенітету в межах кримінального права, є праці, присвячені аналізу окремих аспектів кримінально-правової охорони інформаційної безпеки як складової національної безпеки України, державного суверенітету, або безпосередньо щодо предмета дослідження в межах цього підрозділу – суверенітету в інформаційній сфері[1].

Легальна дефініція інформаційного суверенітету України наразі відсутня[2], що породжує дискусію щодо його змісту та складових.

---

[1] Див., наприклад: Кубальський В. Н. Кримінально-правова охорона державного суверенітету як частина державної політики у сфері протидії злочинності в умовах збройної агресії росії. *Науковий вісник Ужгородського Національного університету. Серія Право.* 2023. Вип. 78. Ч. 2. С. 207–213; Ліпкан В. А., Діордіца І. В. Національна безпека України: кримінально-правова охорона: навч. посіб. К.: КНТ, 2007. С. 253; Олєйніков Д. Зміст та складові інформаційного суверенітету як об'єкта кримінально-правової охорони. *Геополітичні пріоритети України. Збірник наукових праць.* 2021. Вип. 1 (26). С. 60–69; Радутний О. Е. Можливість захисту інформаційного суверенітету України кримінально-правовими засобами. *Інформація і право*. 2014. №3 (12). С. 113–119 та ін.

[2] Хоча до 2011 р. в ст. ст. 53, 54 Закону України «Про інформацію» №2657-XII від 02.10.1992 р. містилися норми, відповідно до яких «основою інформаційного суверенітету України є національні інформаційні ресурси» і були закріплені гарантії інформаційного суверенітету, до яких віднесено: виключне право власності України на інформаційні ресурси, створення національних систем інформації; встановлення режиму доступу інших держав до інформаційних ресурсів України; використання інформаційних ресурсів на основі рівноправного співробітництва з іншими державами, а в ст. 1 Закону України «Про національну програму інформатизації» №74–98-ВР від 04.02.1998 р. (втратив чинність 01.12.2022 р.) інформаційний суверенітет держави визначався, як «здатність держави контролювати і регулювати потоки ін-

Низка науковців здійснюють спробу визначити коло нормативно-правових актів, що, на їх думку, відображають стан правового забезпечення інформаційного суверенітету України[1]. Інші – надають власне бачення розглядуваного поняття, виходячи з загальних нормативних положень, що стосуються державного суверенітету, з урахуванням специфіки, обумовленої інформаційною сферою.

Правовою основою нормативного забезпечення інформаційного суверенітету як складової державного суверенітету, виступає Конституція України та деякі законодавчі акти[2], а також підзаконні, що носять, як правило, декларативний характер[3]. Передусім, у ст. 5 Конституції України проголошено, серед іншого, що носієм суверенітету і єдиним джерелом влади є народ, а також, що право визначати і змінювати конституційний лад належить виключно народові. Тоді стає очевидним, що основою державного суверенітету (у тому числі й суверенітету в інформаційній сфері) виступає народний суверенітет[4]. Відповідно до п. 4.3. мотивувальної частини Рішення КСУ у справі про здійснення влади народом № 6-рп/2005 від 05.10.2005 р. держава, її органи та посадові особи не мають права змінювати конституційний лад. До засад конституційного ладу Конституційний Суд України відніс норми розділів І, ІІІ та ХІІІ Конституції України[5]. Згідно зі ст. 17 Основного Закону (розділ І Конституції України) захист суверенітету і територіальної цілісності

формації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави».

[1] Див., наприклад: Концептуальні основи захисту інформаційного суверенітету України: монографія / О. В. Задерейко, О. В. Троянський, Р. І. Чанишев, А. І. Дика; 2-ге вид., перероб. і доп. Одеса: Фенікс, 2022. С.22–54.

[2] Там само.

[3] Проблеми нормативно-правового забезпечення інформаційного суверенітету: аналітична записка. 2014. *Національний інститут стратегічних досліджень*: вебсайт. URL: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/problemi-normativno-pravovogo-zabezpechennya-informaciynogo (дата звернення: 28.11.2023).

[4] Додатково: розгляд питання про народний суверенітет не є предметом дослідження в даній роботі. Згаданим положенням виключно демонструється, що інформаційний суверенітет держави не є абстракцією, а спирається на принцип народного суверенітету, визначальними характеристиками якого є верховенство та повнота влади народу.

[5] Рішення Конституційного Суду України … (справа про здійснення влади народом) від 5 жовт. 2005 р. № 6-рп/2005. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL : http://zakon4.rada.gov.ua/laws/show/v006p710-05/conv (дата звернення 20.11.2023).

України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. А відповідно до ст. 18 (розділ І) Конституції України зовнішньополітична діяльність України спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права. Крім наведеного, згідно з преамбулою Декларації про державний суверенітет України державний суверенітет України становить верховенство, самостійність, повноту і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах[1].

Певною мірою відображенням саме політико-правової природи та специфіки інформаційного суверенітету є визначення, запропоноване В. О. Олійником, О. В. Сосніним, Л. Є. Шиманським. На думку згаданих дослідників, інформаційний суверенітет Української держави – це виключне право України відповідно до Конституції, законодавства України та норм міжнародного права самостійно і незалежно з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні та геополітичні національні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави[2].

---

[1] Декларація про державний суверенітет України: декларація Верховної Ради Української РСР від 16.07.1990 р. № 55-XII. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/55–12#Text (дата звернення: 08.11.2023).

Дод.: питанню державного суверенітету та його ознак присвячено низку наукових праць, в яких додатково виокремлюють такі ознаки суверенітету, як єдність, невідчужуваність та обумовленість суверенітетом народу (див., наприклад, Куян І. А. Суверенітет: проблеми теорії і практики: конституційно-правовий аспект: монографія. Київ: ВЦ «Академія», 2013. 560 с.; Скрипнюк О. В., Крусян А. Р. Концепт «державний суверенітет у класичних західних теоріях. *Альманах права*. 2021. Вип. 12. С. 11–19 та ін.).

[2] Олійник О. В., Соснін О. В., Шиманський Л. Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. *Держава і право. Юридичні і політичні науки*. 2001. Вип.13. С. 537.

Таким чином, справедливим видається стверджувати, що і в контексті розуміння інформаційного суверенітету як об'єкта кримінально-правової охорони підлягає обов'язковому врахуванню його політико-правова природа. Варто виходити з того, що згідно з ч. 1 ст. 1 КК України «Кримінальний кодекс України має своїм завданням правове забезпечення охорони прав і свобод людини і громадянина, … , конституційного устрою України від кримінально-протиправних посягань, … ». Тож, екстраполюючи вище викладене на інформаційний суверенітет, сформулюємо тезу, що сутність останнього розкривається у таких характеристиках державної влади (яка є похідною від влади народу, але складовою конституційного ладу), як її верховенство, повнота, самостійність, неподільність у забезпеченні формування та реалізації внутрішньої інформаційної політики, а незалежність та рівноправність – у зовнішній політиці в цій сфері. Також справедливим видається вважати, що обидва різновиди політики, юридичною основою реалізації положень яких (передусім, нормативних стосовно протидії інформаційним загрозам) є інформаційний суверенітет, очевидно, мають базуватися на принципах дотримання національних інтересів в інформаційній сфері та забезпечення інформаційної безпеки. Наведені міркування підтверджуються точкою зору В. М. Янка, який зазначив, що забезпечення правової охорони суверенітету є одним з найважливіших завдань КК України. Суверенітет держави поряд з повновладдям Українського народу як носія і єдиного джерела влади в Україні, територіальною цілісністю й недоторканністю державних кордонів виступає необхідною складовою конституційного ладу[1].

Вирішуючи питання про обсяг та зміст кримінально-правової охорони суспільних відносин у царині забезпечення інформаційного суверенітету, варто зазначити, що такі відносини часто не існують «в чистому вигляді», тобто не є такими, що стосуються виключно інформаційного суверенітету. Треба, по-перше, виходити із загальних положень кримінально-правової охорони, а, по-друге, враховувати наукове групування посягань на державний суверенітет, як на родове

[1] Янко В. М. Особливості механізму правового регулювання відносин із забезпечення народного суверенітету: кримінально-правовий аспект. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2018. Вип. 1 (81). С. 141.

стосовно суверенітету інформаційного політико-правове явище. При цьому відправною точкою щодо з'ясування місця інформаційного суверенітету серед інших об'єктів кримінально-правової охорони слугуватиме його дослідження в межах родового об'єкта кримінальних правопорушень, передбачених розділом І Особливої частини КК України[1].

Правильність розгляду інформаційного суверенітету саме як об'єкта кримінально-правової охорони, а не як об'єкта кримінального правопорушення підтверджується такими теоретичними судженнями. Так, такий об'єкт *(йдеться про об'єкт кримінально-правової охорони – прим. автора)* на державному рівні визнаний соціальною цінністю, що ставиться під охорону законодавства про кримінальну відповідальність. Крім того, об'єкт кримінально-правової охорони може охоплювати не лише об'єкт конкретного злочину, а виступати як сукупність цього об'єкта, а також інших об'єктів, пов'язаних з останнім: однорідних основних безпосередніх об'єктів злочинів, додаткових безпосередніх об'єктів як складників інших неоднорідних «поліоб'єктів». Це є характерним, зокрема, для основ національної безпеки, різновидів національної безпеки України (наприклад, громадської безпеки) як об'єктів кримінально-правової охорони[2]. У світлі вище викладеного критично варто ставитися до виокремлення переліків (хоч і не повних) конкретних кримінальних правопорушень, які, на думку авторів, мають своїм об'єктом (видовим чи навіть безпосереднім) суспільні відносини у сфері забезпечення державного чи інформаційного суверенітету[3], хоча, безперечно, такі напрацюван-

---

[1] Федюк В. В. Інформаційний суверенітет як об'єкт кримінально-правової охорони. Актуальні питання у сучасній науці. 2023. № 12 (18). С. 689.

[2] Демидова Л. М. Кримінально-правова охорона національної безпеки України: кримінальна відповідальність за ухилення від проходження служби цивільного захисту в особливий період чи у разі проведення цільової мобілізації: монографія / Л. М. Демидова, В. В. Назарчук; за заг. ред. Л. М. Демидової. Харків: Право, 2019. С. 63.

[3] Див., наприклад, Кубальський В. Н. Засади кримінально-правової охорони державного суверенітету України. *Правова держава: щорічник наукових праць*. Київ, 2015. Вип.26. С. 379; Радутний О. Е. Можливість захисту інформаційного суверенітету України кримінально-правовими засобами. *Інформація і право*. 2014. №3 (12). С. 118–119 та ін.

ня є окресленням предмета подальших ґрунтовних досліджень. Зустрічається й занадто спрощений підхід до показу такого розуміння прояву характеристик суверенітету держави (справедливо й для інформаційного також), чим, з позиції окремих авторів, обумовлюється їх кримінально-правова охорона. Наприклад, «…суверенітет держави, окрім іншого, знаходить своє відображення і в тому, що всі органи державної влади та державного управління в центрі й на місцях вирішують усі питання відповідно до належної компетенції без будь-якого іноземного втручання…»[1] або «…дії, вчинювані безпосередньо проти суверенітету – це дії проти прояву верховної влади на певній території…»[2]. Більш прогресивний підхід, як здається, полягає у групуванні форм кримінально-караних діянь, які посягають на державний суверенітет[3] або за критеріями відповідно до об'єктів посягання і цінностей інформаційного суспільства[4].

Зустрічаються також і міркування, що інформаційний суверенітет вже є об'єктом кримінально-правової охорони (на прикладі розгляду складів правопорушень, передбачених розділом І Особливої частини КК України)[5]. Вважаємо такий напрям розвитку наукової думки перспективним, виходячи з того, що дієвість інформаційного

---

[1] Науково-практичний коментар до Кримінального кодексу України [2-е вид., перероб. та доп.]; за ред. П. П. Андрушка, В. Г. Гончаренка, Є. В. Фесенка. Київ: Дакор, 2008. С. 258.

[2] Рубащенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканність України: монографія. Харків: Право, 2016. С. 54.

[3] Так, О. М. Костенко виокремлює 3 групи норм, які становлять систему кримінально-правової охорони державного суверенітету (за критерієм способу посягання): 1) норми, які охороняють державну владу від узурпації; 2) норми, які охороняють державний суверенітет від діянь, які його ослаблюють; 3) норми, що протидіють зловживанню державною владою і притаманним їй суверенітетом (див. Правове забезпечення державного суверенітету України: монографія / Ю. С. Шемшученко та ін.; за заг. ред. Ю. С. Шемшученка. Київ: Юрид. думка, 2011. С. 234–237).

[4] Такими групами є, зокрема, кібернетична інтервенція (посягання на безпеку кіберпростору держави, авторитет органів державної влади); інформаційна експансія (посягання на інформаційну безпеку, правопорядок держави шляхом використання інформаційного та кіберпростору) (див. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти. Київ: ТОВ «ДКС», 2012. С. 253).

[5] Наприклад, див. Олєйніков Д. Зміст та складові інформаційного суверенітету як об'єкта кримінально-правової охорони. *Геополітичні пріоритети України. Збірник наукових праць.* 2021. Вип. 1 (26). С. 66–67.

суверенітету як частини конституційного ладу – це запорука забезпечення інформаційної безпеки як складової національної безпеки[1]. Враховуючи, що визнання основ національної безпеки України (*не національної безпеки в широкому розумінні, яка охороняється й нормами інших розділів КК – прим. автора)* як родового об'єкта кримінальних правопорушень із розділу І Особливої частини КК України відповідає інтересам суспільства й держави, що особливо проявляється в сучасних умовах першочергової необхідності кримінально-правового захисту незалежності, суверенності, конституційного ладу, територіальної цілісності та територіальної недоторканності нашої держави[2]. Але все одно існує необхідність у додатковому пошуку й інших критеріїв, які можна покласти в основу обґрунтування обсягу кримінально-правової охорони інформаційного суверенітету не лише в межах суспільних відносин у сфері забезпечення основ національної безпеки, а зважаючи на його багату за змістом внутрішню й зовнішню складові.

Такими критеріями (відправною точкою) можуть слугувати національні інтереси України, як визначальні потреби держави Україна. Відповідно до п. 10 ч. 1 ст. 1 Закону України «Про національну безпеку» національні інтереси України – життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує *державний суверенітет України (курсив автора)*, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян[3]. Приміром, якщо конкретизувати, то такими національними інтересами у кібернетичній сфері є: 1) дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації

[1] В межах аналізу родового об'єкта групи норм розділу І КК України таке розуміння інформаційної безпеки є традиційним і усталеним. Хоча, звичайно, існує багато підходів до її визначення. Наприклад, виокремлюють, щонайменше, вісім підходів до розуміння інформаційної безпеки (див. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. С. 33).

2 Актуальні проблеми формування сучасної доктрини кримінального права України : монографія / В. Я. Тацій, Л. М. Демидова, В. І. Борисов та ін.; за заг. ред. В. Я. Тація, Л. М. Демидової, В. І. Борисова. Харків: Право, 2021. С. 334.

[3] Про національну безпеку: Закон України № 2469-VIII від 21.06.2018 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2469–19#Text (дата звернення: 24.11.2023).

та користування нею, сприяння духовному оновленню держав; 2) інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значущих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів; 3) застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації; 4) захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України[1]. Тож, враховуючи, що інтереси завжди більш доступні для дослідження саме тому, що вони мають зовнішній прояв, виступають своєрідним індикатором, що дозволяє в більш зручній формі пізнати ті суспільні відносини, які стоять за ними й приховані від безпосереднього сприйняття[2], визначальним для розкриття сутності інформаційного суверенітету як об'єкта кримінально-правової охорони, в аспекті більш точного окреслення того кола суспільних відносин, які підлягатимуть охороні, виступають саме національні інтереси України в інформаційній (кібер-) сфері.

До того ж саме забезпечення національних інтересів є головною метою (необхідним результатом) державної інформаційної політики, яка здійснюється, передусім, завдяки «…верховенству в комунікаціях у частині мережі Інтернет, яка є національним сегментом мережі, і верховенству у просторі інформаційних ресурсів…»[3]. Зрозуміло, що реалізація принципу верховенства держави у внутрішній сфері інформаційних відносин має здійснюватися на підставі законодавчо встановленої компетенції органів державної влади з урахуванням дотримання прав людини, балансу інтересів особи та суспільства.

[1] Довгань О. Д., Тарасюк А. В. Національні інтереси України в кібернетичній сфері. *Інформація і право.* 2021. № 1 (36). С. 141.

[2] Актуальні проблеми формування сучасної доктрини кримінального права України : монографія / В. Я. Тацій, Л. М. Демидова, В. І. Борисов та ін.; за заг. ред. В. Я. Тація, Л. М. Демидової, В. І. Борисова. Харків: Право, 2021. С. 349.

[3] Ярема О. Г. Зміст інформаційного суверенітету у контексті державного суверенітету. *Юридичний науковий електронний журнал.* 2022. № 3. С. 192.

Так, зокрема, в абз. 4 п. 3 Рішення КСУ №3-р/2021 від 21.12.2021 р. зазначено, що Україна має право захищати свою незалежність, *свій державний суверенітет (курсив автора)* і свою територіальну цілісність шляхом здійснення таких системних заходів і застосування засобів, що є співмірними, допустимими і прийнятними з огляду на рівень небезпеки, загроз і викликів, що постали перед нею[1]. Зазначені критерії особливо підлягають врахуванню при запровадженні кримінальної відповідальності за посягання на окремі складові інформаційного суверенітету.

Тож, інформаційний суверенітет як об'єкт кримінально-правової охорони становить собою складову конституційного ладу, юридичний механізм, а також нормативну основу спрямованості органів державної влади, що діють на підставі Конституції, норм міжнародного права та законів України, виходячи з національних інтересів України, з метою формування та реалізації державної інформаційної політики, спрямованої, серед іншого, на забезпечення інформаційної безпеки як складової національної безпеки України.

2.4. Кримінально-правова охорона інформаційної безпеки дітей

Перехід до інформаційного суспільства позначився на всіх сферах життєдіяльності людства, зокрема, виробничих процесах, сфері дозвілля, міжособистісному спілкуванні, сімейних стосунках, включно з вихованням дітей, та ін. Інформація стала невід'ємною складовою фактично всіх суспільних відносин, а інформаційний простір – щоденним супутником майже кожної людини. Разом із тим у сучасному світі інформація, слугуючи добропорядним громадянам інструментом для отримання знань та вирішення різноманітних завдань, у руках зловмисників може стати засобом для досягнення протиправних цілей.

[1] Рішення Конституційного Суду України у справі №1–252/2018 (3492/18) від 21.12.2021 р. №3-р/2021. *Верховна Рада України. Законодавство України: оф. вебсайт.* URL: https://zakon.rada.gov.ua/laws/show/va03p710-21#Text (дата звернення: 30.11.2023).

Вітчизняна статистика показує постійне збільшення числа кіберзлочинів, тобто суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України[1]. За підрахунками експертів, здійсненими у 2022 р. на підставі аналізу статистики Офісу Генерального прокурора України, лише за останні вісім років на момент підрахунку кількість виявлених кіберзлочинів збільшилась майже в 7,5 разів (без урахування класичних правопорушень із використанням комп'ютерної техніки, а також рівня латентності такої злочинності)[2].

Привабливою та порівняно легкою мішенню для зловмисників, які оперують в інформаційному просторі та використовують інформаційний вплив, можуть бути діти. Це обумовлюється такими загальними особливостями розвитку дітей, як, зокрема: недостатня сформованість навички критичного мислення; довірливість та легкість потрапляння під маніпулятивний вплив; схильність до авантюр та пригод. У зв'язку з цим інформаційна безпека дитини потребує посиленої уваги й охорони держави й суспільства. Одним із важливих засобів охорони дітей від інформаційних небезпек виступає кримінальна відповідальність.

Щодо поширеності кримінальних правопорушень проти дітей, пов'язаних із інформаційним впливом або вчинених в інформаційному полі, слід також відмітити тенденцію до їх невпинного зростання, на що впливають такі фактори, як розвиток та поширення цифрових технологій, цифровізація усіх суспільних процесів, поширення інформаційної залежності, залежності від гаджетів. Одним із прискорювачів таких процесів стала пандемія COVID-19, яка зумовила перехід зловмисників у цифровий простір із метою вчинення суспільно

[1] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

[2] Єрема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *LIGA ZAKON*: оф. вебсайт. URL: https://jurliga.ligazakon.net/analitycs/210562_ borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-21–49-ix

небезпечних посягань. Дистанційне навчання, збільшення проведення часу в інтернеті, використання соціальних мереж і чатів підвищило для дітей ризики стати жертвами різноманітних правопорушень[1].

Сучасний стан регламентації кримінальної відповідальності за кримінальні правопорушення, що посягають на інформаційну безпеку дітей.

Здійснюючи огляд сучасного стану регламентації кримінальної відповідальності за кримінальні правопорушення, що посягають або можуть посягати на інформаційну безпеку дітей, варто зауважити, що норми, які передбачають кримінальну відповідальність за відповідні діяння, розміщені в різних розділах Особливої частини КК: у першому («Злочини проти основ національної безпеки України»), у другому («Кримінальні правопорушення проти життя та здоров'я особи»), третьому («Кримінальні правопорушення проти волі, честі та гідності особи»), четвертому («Кримінальні правопорушення проти статевої свободи та статевої недоторканості особи»), п'ятому («Кримінальні правопорушення проти виборчих, трудових та інших особистих прав і свобод людини і громадянина»), шостому («Кримінальні правопорушення проти власності»), дванадцятому («Кримінальні правопорушення проти громадського порядку та моральності»), тринадцятому («Кримінальні правопорушення у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші кримінальні правопорушення проти здоров'я населення»), шістнадцятому («Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку») розділах.

У попередніх дослідженнях кримінально-правової охорони дитинства нами виділялися *рівні кримінально-правового забезпечення*

[1] Куковинець Д. О. Захист дітей від сексуальної експлуатації та сексуального насильства в Інтернеті в умовах пандемії COVID-19: до питання домагання дитини для сексуальних цілей. *Питання боротьби зі злочинністю* : зб. наук. пр. / редкол.: В. С. Батиргареєва (голов. ред.) та ін. Харків : Право, 2021. Вип. 42. С. 74–83. URL: http://pbz.nlu.edu.ua/article/view/252033. С. 75.

*охорони сім'ї, опіки, піклування та нормального розвитку дітей (*за критерієм їх конкретизованості)*: загальний, спеціальний, особливий та окремий*[1]. Крізь призму таких рівнів також можливо виразити й кримінально-правову охорону інформаційної безпеки дітей.

На *загальному рівні* охорона інформаційної безпеки дітей виражається в загальних кримінально-правових нормах, де потерпілою особою може виступати будь-яка особа безвідносно віку (як повнолітня особа, так і неповнолітня або малолітня особа). При цьому, якщо кваліфікація відбувається за такими нормами, суд обов'язково обтяжує покарання у разі вчинення кримінального правопорушення щодо малолітньої дитини або у присутності дитини (п. 6 ч. 1 ст. 67 КК).

До норм загального рівня, передбачені якими діяння посягають на інформаційну безпеку дітей, належать, наприклад: ч. 3 ст. 111[1] КК – дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти; ст. 129 КК – погроза вбивством; ст. 145 – незаконне розголошення лікарської таємниці; ст. 163 – порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер; ст. 176 – порушення авторського права і суміжних прав; ст. 182 – порушення недоторканності приватного життя; ст. 189 – вимагання; ст. 190 – шахрайство; ст. 361 – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, та ін.

Спеціальний рівень виражається у нормах, виділених у межах загальних кримінально-правових норм, в яких містяться обставини, що обтяжують кримінальну відповідальність за вчинення правопо-

[1] Євтєєва Д. П. До питання про рівні кримінально-правового забезпечення охорони сім'ї, дітей та підопічних в Україні. *Вісник Асоціації кримінального права України*. 2018. Вип. 1 (10). С. 107–115. URL: http://nauka.nlu.edu.ua/wp-content/uploads/2018/07/09_Evteeva.pdf; Євтєєва Д. П. Доктринальні проблеми кримінальної відповідальності за правопорушення у сфері сім'ї, опіки, піклування та нормального розвитку дітей / Актуальні проблеми формування сучасної доктрини кримінального права України : монографія / В. Я. Тацій, Л. М. Демидова, В. І. Борисов та ін. ; за заг. ред. В. Я. Тація, Л. М. Демидової, В. І. Борисова. Харків : Право, 2021. 632 с. С. 305–310. URL: http://surl.li/cyikb.

рушення щодо дитини, із примушуванням, втягненням чи залученням дитини до вчинення окремих діянь або заняття певною діяльністю.

Прикладом таких норм із правопорушеннями проти інформаційної безпеки власне дітей можуть бути:

• ст. 120 КК – доведення до самогубства (ч. 3 – щодо неповнолітнього);

• ст. 151^2 КК – примушування до шлюбу (щодо особи, яка не досягла шлюбного віку (ч. 2);

• ст. 300 КК – ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ч. 2 – збут неповнолітнім чи розповсюдження серед них творів; ч. 3 – примушування неповнолітніх до участі у створенні творів);

• ст. 301 КК – ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ч. 2 – збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру);

• ст. 302 КК – створення або утримання місць розпусти і звідництво із залученням неповнолітнього (ч. 2) або малолітнього (ч. 3);

• ст. 303 КК – сутенерство або втягнення особи в заняття проституцією (ч. 3 щодо неповнолітнього, ч. 4 – щодо малолітнього);

• ст. 307 КК – незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ч. 2 – із залученням неповнолітнього, а також збут наркотичних засобів, психотропних речовин або їх аналогів у місцях, що призначені для проведення навчальних, спортивних і культурних заходів; ч. 3 – вчинені із залученням малолітнього або щодо малолітнього);

• ст. 309 КК – незаконне виробництво, виготовлення, придбання, зберігання, перевезення чи пересилання наркотичних засобів, психотропних речовин або їх аналогів без мети збуту (дії, передбачені частинами першою або другою цієї статті, вчинені із залученням неповнолітнього);

• ст. 315 КК – схиляння до вживання наркотичних засобів, психотропних речовин або їх аналогів (ч. 2 – та сама дія, вчинена щодо неповнолітнього).

Особливий рівень набуває прояв в охороні інформаційної безпеки дітей у самостійних кримінально-правових нормах. При цьому вони є спеціальними щодо інших норм Особливої частини КК й за відсутності перших ті або інші діяння кваліфікувалися б за другими, у зв'язку з чим відповідні суспільні відносини не втратили б кримінально-правової охорони.

До таких норм належить, приміром:

• ст. 168 КК України (розголошення таємниці усиновлення (удочеріння), стосовно якої загальною є нормою ст. 182 КК (порушення недоторканності приватного життя);

• ст. 156^1 КК (домагання дитини для сексуальних цілей), стосовно якої загальними нормами виступають інші норми Розділу IV Особливої частини КК «Кримінальні правопорушення проти статевої свободи та статевої недоторканості особи» у статтях 152, 153, 154, 155 та 156;

• норми в ч. 2–4 ст. 301^1 КК (ввезення в Україну дитячої порнографії з метою збуту чи розповсюдження або її зберігання, перевезення чи інше переміщення з тією самою метою; виготовлення, розповсюдження, збут дитячої порнографії або примушування неповнолітньої особи до участі у створенні дитячої порнографії) є спеціальними щодо норми в ст. 301 КК «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів».

Окремий рівень виражається в самостійних кримінально-правових нормах, які, на відміну від особливого рівня, не співвідносяться з іншими нормами КК як спеціальні із загальними у чистому вигляді, наприклад:

• ст. 126^1 КК – домашнє насильство (психологічне);

• ст. 156 КК – розбещення неповнолітніх (інтелектуальне);

• ч. 1 ст. 301^1 КК – умисне одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій або умисне її придбання, або умисне зберігання, ввезення в Україну, перевезення чи інше переміщення дитячої порнографії без мети збуту чи розповсюдження;

• ст. 301^2 КК – проведення видовищного заходу сексуального характеру за участю неповнолітньої особи;

• ст. 304 КК – втягнення неповнолітніх у протиправну діяльність.

Таким чином, кримінально-правова охорона інформаційної безпеки дітей виражається в сукупності кримінально-правових норм, в яких закріплено відповідальність за посягання на життя та здоров'я дітей, їх волю, честь та гідність, власність, нормальний розвиток від негативного інформаційного впливу, інших операцій із інформацією, незаконного використання інформаційно-комунікаційних систем, а також незаконних дій інших осіб із інформацією з обмеженим доступом.

Тенденції розвитку законодавчої регламентації кримінально-правової охорони інформаційної безпеки дітей.

Протягом останніх років законодавець приділяє значну увагу посиленню охорони інформаційної безпеки, у т. ч. й інформаційної безпеки дітей, зокрема й на кримінально-правовому рівні. Оскільки інформаційні відносини розвиваються надзвичайно швидко, законодавець здійснює постійний моніторинг небезпечних проявів в інформаційній сфері та у разі заподіяння або створення загрози заподіяння такими проявами істотної шкоди правам та інтересам громадян вводить відповідні заходи відповідальності, у т. ч. й кримінальної.

Так, у 2018 р., ГО «Ла Страда Україна» оприлюднила статистику звернень за допомогою через онлайн-небезпеку, що стосувалася дітей. Загалом таких звернень за півтора року було більше 11,4 тис., із яких:

• щодо комп'ютерної та інтернет залежності – 2877;

• щодо секстингу (інтимне листування й пересилка фото інтимного характеру) – 2627;

• щодо тролінгу (глузування з дитини та провокацій щодо неї) – 1532;

• щодо фішингу (інтернет-шахрайство, метою якого є отримати доступ до логінів та паролів користувача) – 1207;

• щодо грумінгу (входження в довіру до дитини з метою подальшої особистої зустрічі для вступу в сексуальні відносини, експлуатації чи шантажу) – 1047;

• щодо смертельних квестів в соціальних мережах – 919;

• щодо мобінгу (цькування групою людей) – 697;

• щодо кібербулінгу (цькування дитини онлайн) – 398;

• щодо кардингу (шахрайство з банківськими картками) – 122[1].

На сьогодні законодавець вжив заходів щодо протидії зазначеним видам небезпек, ввівши кримінальну відповідальність за низку зазначених проявів (за секстинг, грумінг, смертельні квести, частково кібербулінг (якщо останні призвели до самогубства). Стосовно ж таких дій, як фішинг і кардинг, можна констатувати, що вони з моменту своєї появи уже охоплювалися ст. 190 Кримінального кодексу України (далі – КК України) (шахрайство).

Загалом за останні шість років можна відмітити тенденцію посилення кримінально-правової охорони інформаційної безпеки дітей у виді запровадження відповідальності за певні суспільно небезпечні прояви шляхом введення до КК України нових норм або ж внесення змін до чинних його норм. Відповідні новели переважно. стали наслідком імплементації у вітчизняне законодавство таких міжнародних актів, як Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу з цими явищами (Закон України від 06.12.2017 р. № 2227-VIII) [2] та Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротська Конвенція) (Закон України від 18.02.2021 р. № 1256-IX)[3]. Зокрема, набули криміналізації:

• доведення особи до самогубства або до замаху на самогубство, що є наслідком систематичного протиправного примусу до дій, що суперечать її волі, схиляння до самогубства, а також інших дій, що сприяють вчиненню самогубства (ч. 1 ст. 120 КК України, 2018-й р.);

---

[1] Толокольнікова К. Секстинг, грумінг, мобінг: від чого страждають діти в інтернеті. *Дім media sapiens*: вебсайт. URL: https://ms.detector.media/media-i-diti/post/21656/2018-08-20-sekstyng-gruming-mobing-vid-chogo-strazhdayut-dity-v-interneti/

[2] Про внесення змін до Кримінального та Кримінального процесуального кодексів України з метою реалізації положень Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу з цими явищами: Закон України від 06.12.2017 р. № 2227-VIII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: http://zakon5.rada.gov.ua/laws/show/2227–19.

[3] Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції): Закон України від 18.02.2021 р. № 1256-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/1256–20#n24.

• домашнє насильство, у т. ч. й психологічне (ст. 126^1 КК України, 2017-й р., вступила в силу в 2019-му р.);

• примушування до шлюбу (ст. 151^2 КК України, 2017-й р., вступила в силу в 2019-му р.);

• домагання дитини для сексуальних цілей (ст. 156^1 КК України, 2021-й р.);

• одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ст. 301^1 КК України, 2021-й р.);

• проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ст. 301^2 КК України, 2021-й р.);

• дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти (ч. 3 ст. 111^1 КК України, 2022-й р.).

Загальна характеристика кримінальних правопорушень, що посягають на інформаційну безпеку дітей.

Характеризуючи кримінальні правопорушення, що посягають на інформаційну безпеку дітей, слід відмітити, що, на нашу думку, інформаційна безпека може претендувати на визнання її *об'єктом кримінального правопорушення* у відповідних посяганнях. Зокрема, *основним об'єктом її можливо визнати у таких правопорушеннях, як* перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку – ст. 363^1 КК України; порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер – ст. 163 КК України. У свою чергу, *додатковим об'єктом* інформаційну безпеку можливо визнати в таких кримінальних правопорушеннях: спонукання неповнолітніх до застосування допінгу – ст. 323 КК України; домагання дитини для сексуальних цілей – ст. 156^1 КК України (обов'язковий об'єкт); домашнє насильство (психологічне) – ст. 126^1 КК України, розбещення неповнолітніх (в інтелектуальній формі) – ст. 156 КК України (факультативний об'єкт).

Власне ж інформація може бути предметом розглядуваних кримінальних правопорушень (якщо це передбачено або безпосередньо

випливає з тієї чи іншої норми КК України) або ж, виступаючи інструментом впливу або досягнення протиправної мети, бути пов'язаною з діянням, способом його вчинення або іншими ознаками.

Як *предмет* у кримінальних правопорушеннях, що посягають на інформаційну безпеку дітей, інформація виступає як відомості з обмеженим доступом у виді, зокрема, таємниці усиновлення (ст. 168 КК України), таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК України), лікарської таємниці (ст. 145 КК України). Окрім того, на наш погляд, інформація цілком могла б претендувати на визнання її предметом низки інших кримінальних правопорушень, що посягають на інформаційну безпеку дітей, в яких наразі таким предметом вважаються інші речі матеріального світу, з якими, однак, вона тісно пов'язана і фактично виступає їх ядром (сутністю). Зокрема, мова йде про твори науки, літератури, мистецтва та інших об'єктів авторського права і суміжних прав (ст. 176 КК України), твори, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300 КК України), твори, зображення або інші предмети порнографічного характеру (ст. 301 КК України), матеріали дитячої порнографії (ст. 301^1 КК України), шкідливі програмні засоби, призначені для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361^1 КК України). Зазначені твори або інші матеріали виступають формою вираження певної інформації в аудіо-, відео-, текстовому, графічному або іншому форматі, при цьому зазначена інформація охороняється законодавством або навпаки становить небезпеку для суспільства. Разом із тим слід зауважити, що положення щодо визнання інформації до предмета кримінального правопорушення в цих випадках висловлене як гіпотеза, що потребує подальшої більш ґрунтовної окремої наукової розробки.

Характеризуючи *діяння* у кримінальних правопорушеннях проти інформаційної безпеки дітей, можна стверджувати, що вони передбачають активні дії та є різноманітними за характером. Водночас

варто відзначити, що деякі діяння можуть бути пов'язані з незаконними операціями з інформацією, інформаційними технологіями або інформаційним впливом. Зокрема:

– при розголошенні таємниці усиновлення (ст. 168 КК України), незаконному розголошенні лікарської таємниці (ст. 145 КК України) відбувається несанкціоноване поширення, використання інформації з обмеженим доступом;

– при розповсюдженні або збуті шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 363^1 КК України) має місце протиправне застосування інформаційних технологій;

– при погрозі вбивством (ст. 129 КК України), психологічному домашньому насильстві (ст. 126^1 КК України), схилянні неповнолітнього до вживання наркотичних засобів, психотропних речовин або їх аналогів (ч. 2 ст. 315 КК України), спонуканні неповнолітніх до вживання допінгу (ст. 323 КК України), схилянні неповнолітніх до вживання одурманюючих засобів (ст. 324 КК України) відбувається негативний інформаційний вплив.

Іще однією ознакою кримінальних правопорушень проти інформаційної безпеки дітей може бути *спосіб їх вчинення,* який може виступати як їх обов'язковою ознакою, так і факультативною. При цьому в одних випадках він тісно пов'язаний із діянням (наприклад, при різних проявах втягнення неповнолітніх у протиправну діяльність (ст. 304, ч. 3 ст. 300, ч. 3 ст. 301, ч. 3 ст. 302, ч. 3 ст. 303, ч. 3 ст. 307, ч. 3 ст. 309, ч. 2 ст. 315, ч. 2 ст. 317, ст. 323, ст. 324 КК України), а в інших має більш виражене самостійне значення. Конкретні способи можуть виявлятися в:

– несанкціонованому поширенні, використанні інформації з обмеженим доступом (наприклад, погроза розголошення відомостей, які потерпілий бажає зберегти в таємниці, при вимаганні (ст. 189 КК України);

– неповному або невірогідному використанні інформації (наприклад, застосування обману при шахрайстві (ст. 190 КК України);

– у застосуванні інформаційних технологій (наприклад, розбещення неповнолітніх шляхом використання соцмереж (ст. 156 КК України), використання інформаційно-телекомунікаційних систем або технологій при домаганні дитини для сексуальних цілей (ст. 156[1] КК України), вчинення шахрайства за допомогою інформаційно-комунікаційних систем (ст. 190 КК України), використання інформаційно-телекомунікаційних систем або технологій при умисному одержанні доступу до дитячої порнографії (ст. 301[1] КК України), втягнення неповнолітніх у протиправну діяльність із використанням месенджерів (ст. 304 КК України та спеціальні щодо неї норми), збут неповнолітньому наркотичних засобів через їх продаж у мережі Інтернет (ст. 307 КК України) та ін.);

– негативному інформаційному впливі (наприклад, умовляння, переконання, погрози тощо при втягненні неповнолітнього у протиправну діяльність (ст. 304 КК України та спеціальні щодо неї норми).

За конструкцією склади кримінальних правопорушень проти інформаційної безпеки дітей можуть бути матеріальними (шахрайство – ст. 190 КК України), формальними (вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку – ст. 155 КК України, розголошення таємниці усиновлення – ст. 168 КК України) або усіченими (погроза вбивством – ст. 129 КК України, залучення неповнолітнього до незаконного придбання наркотичних засобів з метою збуту (ч. 2 ст. 307 КК України).

Стосовно *наслідків* розглядуваних кримінальних правопорушень, вони можуть виступати як обов'язкова ознака складу, або ж перебувати поза його межами, та виражатися у шкоді дитині, обумовленій застосуванням інформаційних технологій, негативним інформаційним впливом, недостовірному використанні інформації, несанкціонованому розповсюдженні, використанні й порушенні цілісності, конфіденційності та доступності інформації. Конкретна шкода дитині може виражатися у:

– *фізичній шкоді:* шкоді життю, здоров'ю дитині (наприклад, доведення до самогубства внаслідок систематичного приниження її гідності; розлад здоров'я внаслідок психологічного домашнього насильства);

– *майновій шкоді:* втрата коштів або майна внаслідок шахрайських дій;

– *шкоді нормальному розвитку дитини* – духовному, психічному, інтелектуальному, соціальному (наприклад, шкода психічному й соціальному розвитку дитини від розбещення, вчиненого шляхом дій інформаційного характеру; шкода розвитку дитини за багатьма аспектами від втягнення у протиправну діяльність).

За наявності наслідків як обов'язкової ознаки складу важливе значення набуває встановлення *причинного зв'язку* між ними та діянням.

За *суб'єктивною стороною* розглядувані правопорушення вчиняються з прямим умислом. Особа усвідомлює характер та суспільну небезпеку своїх дій, передбачає суспільно небезпечні наслідки свого діяння та бажає їх настання. Мотиви та цілі при цьому можуть бути різними.

Що стосується суб'єкта розглядуваних кримінальних правопорушень, він може бути загальним або спеціальним. Серед спеціальних суб'єктів, зокрема –батько, матір, вітчим, мачуха, член сім'ї чи близький родич, опікун чи піклувальник, або особа, на яку покладено обов'язки щодо виховання потерпілого чи піклування про нього. У зв'язку з покладеними на зазначених осіб обов'язками щодо виховання дітей в низці норм КК України за кримінальні правопорушення, що посягають на інформаційну безпеку дітей, зазначені особи несуть посилену кримінальну відповідальність (статті 155 КК України (вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку), ст. 156 КК України (вчинення розпусних дій щодо особи, яка не досягла шістнадцятирічного віку), ст. 304 КК України (втягнення неповнолітніх у протиправну діяльність), ст. 323 КК України (спонукання неповнолітніх до застосування допінгу).

Насамкінець слід відзначити, що в проблематиці кримінально-правової охорони інформаційної безпеки дітей виділяються безліч нагальних питань. Зокрема, керуючись безпосередніми об'єктами посягання, можливо виокремити проблеми кримінально-правової охорони інформаційної безпеки життя та здоров'я дітей, їх волі, чес-

ті та гідності, нормального морального розвитку, статевого розвитку та ін. У рамках цих блоків питання є чисельними та різноманітними й вимагають подальших предметних розробок для напрацювання пропозицій щодо їх вирішення.

За результатами цього дослідження можна зробити такі висновки.

1. У кримінально-правовій охороні інформаційної безпеки дітей можливо виділити такі рівні за критерієм їх конкретизованості, як загальний, спеціальний, особливий та окремий.

На загальному рівні охорона інформаційної безпеки дітей виражається в загальних кримінально-правових нормах, де потерпілою особою може виступати будь-яка особа безвідносно віку (ст. 145 КК України – незаконне розголошення лікарської таємниці). Спеціальний рівень виражається у нормах, виділених у межах загальних кримінально-правових норм, в яких містяться обставини, що обтяжують кримінальну відповідальність за вчинення правопорушення щодо дитини, із примушуванням, втягненням чи залученням дитини до вчинення окремих діянь або заняття певною діяльністю (ст. 120 КК України – доведення до самогубства (ч. 3 – щодо неповнолітнього). Особливий рівень набуває прояв в охороні інформаційної безпеки дітей у самостійних кримінально-правових нормах, які є спеціальними щодо інших норм Особливої частини КК (наприклад, ст. 168 КК України (розголошення таємниці усиновлення (удочеріння), стосовно якої загальною нормою є ст. 182 КК України (порушення недоторканності приватного життя). Окремий рівень виражається в самостійних кримінально-правових нормах, які, на відміну від особливого рівня, не співвідносяться з іншими нормами КК як спеціальні із загальними у чистому вигляді (наприклад, ст. 156 КК України – розбещення неповнолітніх (інтелектуальне).

Кримінально-правова охорона інформаційної безпеки дітей виражається в сукупності кримінально-правових норм, в яких закріплено відповідальність за посягання на життя та здоров'я дітей, їх волю, честь та гідність, власність, нормальний розвиток від негативного інформаційного впливу, інших операцій із інформацією, незаконного використання інформаційно-комунікаційних систем, а також незаконних дій інших осіб із інформацією з обмеженим доступом.

2. За останні шість років можна відмітити тенденцію посилення кримінально-правової охорони інформаційної безпеки дітей у виді

запровадження відповідальності за певні суспільно небезпечні прояви шляхом введення до КК України нових норм або ж внесення змін до чинних його норм. Зокрема, набули криміналізації: доведення особи до самогубства або до замаху на самогубство, що є наслідком систематичного протиправного примусу до дій, що суперечать її волі, схиляння до самогубства, а також інших дій, що сприяють вчиненню самогубства (ч. 1 ст. 120 КК України); домашнє насильство, у т. ч. й психологічне (ст.126[1] КК України); примушування до шлюбу; домагання дитини для сексуальних цілей (ст. 156[1] КК України) та ін.

3. Інформаційна безпека може претендувати на визнання її об'єктом кримінального правопорушення у відповідних посяганнях (основним або додатковим). Власне ж інформація може бути предметом розглядуваних кримінальних правопорушень або ж, виступаючи інструментом впливу або досягнення протиправної мети, бути пов'язаною з діянням, способом його вчинення або іншими ознаками.

Як предмет у кримінальних правопорушеннях, що посягають на інформаційну безпеку дітей, інформація виступає як відомості з обмеженим доступом у виді, зокрема, таємниці усиновлення (ст. 168 КК). Разом із тим як гіпотеза висувається положення, що інформація може претендувати на визнання її предметом низки інших кримінальних правопорушень, що посягають на інформаційну безпеку дітей, в яких наразі таким предметом вважаються інші речі матеріального світу (приміром, твори науки, літератури, мистецтва та інших об'єктів авторського права і суміжних прав (ст. 176 КК), з якими, однак, інформація тісно пов'язана й фактично виступає їх ядром (сутністю).

Діяння у кримінальних правопорушеннях проти інформаційної безпеки дітей передбачають активні дії та є різноманітними за характером. При цьому деякі діяння можуть бути пов'язані з несанкціонованим поширенням, використанням інформації з обмеженим доступом, протиправним застосування інформаційних технологій або негативним інформаційним впливом.

Ознакою кримінальних правопорушень проти інформаційної безпеки дітей може бути спосіб їх вчинення, який може виступати як їх обов'язковою ознакою, так і факультативною. Конкретні способи можуть виявлятися в несанкціонованому поширенні, використанні інформації з обмеженим доступом, неповному або невірогідному ви-

користанні інформації, застосуванні інформаційних технологій, негативному інформаційному впливі.

За конструкцією склади кримінальних правопорушень проти інформаційної безпеки дітей можуть бути матеріальними, формальними або усіченими. Наслідки кримінальних правопорушень проти інформаційної безпеки дітей можуть виступати як обов'язкова ознака того чи іншого складу, або ж перебувати поза його межами, та виражатися у фізичній шкоді, майновій шкоді або шкоді нормальному розвитку дитини (духовному, психічному, інтелектуальному, соціальному). За наявності наслідків як обов'язкової ознаки складу важливе значення набуває встановлення причинного зв'язку між ними та діянням.

За суб'єктивною стороною розглядувані правопорушення вчиняються з прямим умислом. Мотиви та цілі при цьому можуть бути різними.

Суб'єкт цих кримінальних правопорушень може бути загальним або спеціальним. Серед спеціальних суб'єктів, зокрема – батько, матір, вітчим, мачуха, член сім'ї чи близький родич, опікун чи піклувальник, або особа, на яку покладено обов'язки щодо виховання потерпілого чи піклування про нього. У низці норм КК України за кримінальні правопорушення, що посягають на інформаційну безпеку дітей, зазначені особи несуть посилену кримінальну відповідальність.

2.5. Караність кримінальних правопорушень проти інформаційної безпеки держави за кримінальним законодавством України

Спеціальні інформаційні операції та кіберзлочини стали невід'ємною складовою сучасної війни. З початком повномасштабного вторгнення рф в Україну суттєво збільшилася кількість злочинних посягань на інформаційну безпеку нашої країни, що актуалізувало дослідження кримінальних правопорушень у цій сфері, метою яких

є удосконалення кримінально-правового регулювання. Одним із напрямів таких досліджень стали питання караності кримінальних правопорушень проти інформаційної безпеки та ефективності передбачених кримінальним законодавством санкцій.

Загальновідомо, що належна кримінально-правова охорона будь-яких цінностей, у тому числі й таких, як інформаційна безпека, забезпечується тільки тоді, коли створені й застосовані ефективні кримінально-правові засоби. Не виникає жодних сумнівів стосовно того, що головним кримінально-правовим засобом охорони суспільних цінностей є кримінальна відповідальність, головною складовою якої є покарання.

Традицією вітчизняного законодавства, як і законодавства більшості європейських держав, є встановлення конкретних видів і розмірів покарань за вчинення окремих кримінальних правопорушень у санкціях відповідних статей Особливої частини КК України. Таким чином, саме санкції статей Особливої частини КК і вміщують у собі основний зміст кримінально-правових засобів, за допомогою яких здійснюється охорона тих соціальних цінностей, на які посягають кримінальні правопорушення[1].

Перш ніж розпочати дослідження караності кримінальних правопорушень проти інформаційної безпеки держави, необхідно визначити, які склади кримінальних правопорушень посягають на зазначений об'єкт суспільних відносин.

На підставі визначення інформаційної безпеки згідно з положеннями Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28.12.2021 № 685/2021[2], що надавалось у підрозд. 1.1., можна зробити висновок, що інформаційна безпека держави є комплексним явищем, яке включає в себе, зокрема, захист інформаційного простору держави від негативних інформаційних впливів, безпеку інформаційно-комунікаційних систем, в яких об-

[1] Новікова К. А. Деякі питання караності злочинів проти життя та здоров'я особи. *Вісник Асоціації кримінального права України*. 2016. №2 (7). С.187–201.

[2] Про Стратегію інформаційної безпеки: Указ Президента України Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

робляється та зберігається інформація, а також захищеність суспільно-важливої інформації з обмеженим доступом.

У чинному КК України відсутній окремий розділ, яким охоплюються кримінальні правопорушення проти інформаційної безпеки, що значно ускладнює виокремлення вичерпного переліку таких правопорушень. Необхідність дослідження караності кримінальних правопорушень проти інформаційної безпеки та наведене визначення «інформаційної безпеки» дають підстави вирізнити три групи кримінальних правопорушень, які на неї посягають.

До ***першої групи*** належать кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Інформаційна безпека є родовим об'єктом цих правопорушень. Ця група включає всі кримінальні правопорушення, передбачені розділом XVI Особливої частини КК України: ст.ст. 361 («Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»), 361^1 («Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»), 361^2 («Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»), 362 («Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»), 363 («Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється») та 363^1 («Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку») КК України.

Треба зауважити, що зазначені правопорушення будуть розглядатися як такі, що посягають на інформаційну безпеку держави, лише у тому випадку, якщо вони спрямовані на об'єкти критичної інфраструктури та інформаційно-телекомунікаційні системи, в яких обробляється суспільно-важлива інформація з обмеженим доступом (державна таємниця тощо). Якщо ж об'єктом посягання буде приватна інформаційно-телекомунікаційна система, то відсутні підстави віднесення цих правопорушень до посягань на інформаційну безпеку саме держави.

До ***другої групи*** кримінальних правопорушень проти інформаційної безпеки належать правопорушення, що посягають на суспільні відносини у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави. Ця група включає такі склади кримінальних правопорушень як: ст.ст. 111 («Державна зрада») – у частині шпигунства, 114 («Шпигунство»), 114^2 («Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану»), 328 («Розголошення державної таємниці»), 329 («Втрата документів, що містять державну таємницю»), 330 («Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни») – в частині інформації зібраної у процесі контррозвідувальної діяльності та у сфері оборони країни, та 422 («Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості») КК України.

До ***третьої групи*** кримінальних правопорушень проти інформаційної безпеки держави належать ті, що посягають на інформаційний простір держави. Ця група включає такі склади кримінальних правопорушень як: ст.ст. 109 («Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади») – у частині публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення дер-

жавної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, 110 («Посягання на територіальну цілісність і недоторканність України») – у частині публічних закликів чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України, 111^1 («Колабораційна діяльність»), а саме ч. 1 («Публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики громадянином України до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України»), ч. 3 («Здійснення громадянином України пропаганди у закладах освіти незалежно від типів та форм власності з метою сприяння здійсненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України, а також дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти») та ч. 6 («Організація та проведення заходів політичного характеру, здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України, за відсутності ознак державної зради, активна участь у таких заходах») – у частині здійснення інформаційної діяльності у співпраці з державою-агресором, цієї статті, 436 («Пропаганда війни»), 436^1 («Виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів») та 436^2 («Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників») КК України.

Як вбачається, кримінальні правопорушення проти інформаційної безпеки держави розміщені у низці розділів Особливої частини КК України («Злочини проти основ національної безпеки», «Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації», «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» «Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку»), але об'єднані таким об'єктом посягання як інформаційна безпека.

Отже, визначившись з переліком кримінальних правопорушень проти інформаційної безпеки перейду до аналізу їх караності.

Щодо *першої групи* досліджуваних правопорушень, то всього у розділі XVI («Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку») передбачено шість статей та п'ятнадцять кримінальних правопорушень і санкцій за ці правопорушення. Серед них чотири санкції (26,7%) встановлено за проступок, сім (46,7%) – за нетяжкі злочини, дві (13,3%) – за тяжкі злочини, і дві (13,3%) – за особливо тяжкі злочини. Дев'ять санкцій – є альтернативними, шість – безальтернативні.

Штраф передбачено восьма санкціями, виправні роботи – двома, обмеження волі містять п'ять санкцій, позбавлення волі – одинадцять. Всі санкції є відносновизначеними. Дві санкції містять додаткове покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю, яке суд може застосувати, або прийняти рішення щодо незастосовування (кумулятивні санкції з альтернативним покаранням), п'ять санкцій – позбавлення права обіймати певні посади або займатися певною діяльністю як безальтернативне покарання (кумулятивна санкція).

Для визначення практики застосування зазначених покарань проаналізована судова статистика за 2021 та 2022 рр.

Загальна кількість засуджених за ці кримінальні правопорушення у 2021 р. становить 76 осіб, тоді як за 2022 р. – 74 особи. Позбавлення волі у 2021 р. призначалось 8 разів, у тому числі у розмірах понад

1 рік до 2 років включно – 2, понад 2 роки до 3 років включно – 4, понад 3 роки до 5 років включно – 1, понад 5 років до 10 років включно – 1, обмеження волі – 3 рази, штраф – 26 разів. 39 осіб було звільнено від відбування покарання з випробуванням. Додаткові покарання були призначені 17 разів (1 раз – штраф, 16 – позбавлення права обіймати певні посади або займатися певною діяльністю). Цікаво, що суд призначив штраф як додаткове покарання за ч. 3 ст. 362 КК України, тоді як санкція не містить додаткового покарання у виді штрафу, що суперечить ч. 3 ст. 53 КК України.

У 2022 р. позбавлення волі призначалося 10 разів, у тому числі в розмірах понад 1 рік до 2 років включно – 1, понад 2 роки до 3 років включно – 7, понад 3 роки до 5 років включно – 2, обмеження волі – 2 рази, виправні роботи – 1 і штраф – 23 рази. 38 осіб було звільнено від відбування покарання з випробуванням і 20 разів призначалося додаткове покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю.

Щодо *другої групи* кримінальних правопорушень проти інформаційної безпеки, то вона включає шість статей та тринадцять кримінальних правопорушень і санкцій за ці правопорушення[1]. З них – сім санкцій (53,8%) встановлено за нетяжкі правопорушення, чотири – за тяжкі (30,8%), і дві (15,4%) – за особливо тяжкі правопорушення. Дванадцять санкцій є безальтернативними і лише одна – альтернативна.

Позбавлення волі передбачено у всіх тринадцяти санкціях, обмеження волі – у двох санкціях. Всі санкції є відносновизначеними. Одна санкція містить конфіскацію майна як додаткове покарання, яке суд може застосувати або ні (кумулятивні санкції з альтернативним покаранням), три санкції – альтернативні додаткові покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю. Одна передбачає позбавлення права обіймати певні посади або займатися певною діяльністю як безальтернативне додаткове покарання.

[1] При аналізі не досліджувалася державна зрада (ст. 111 КК України), у зв'язку з тим, що не всі форми об'єктивної сторони переважно посягають на інформаційну безпеку держави.

Щодо практики застосування покарання за 2021 та 2022 рр. можна сказати таке. Загальна кількість засуджених за ці правопорушення складає 3 – у 2021 р., 33 – у 2022 р.

У 2021 р. – двом особам призначений штраф, одна особа – звільнена від відбування покарання з випробуванням. У 2022 р. позбавлення волі призначалося 13 разів, у тому числі в розмірах понад 1 рік до 2 років включно – 4, понад 3 роки до 5 років включно – 4, понад 5 років до 10 років включно – 5 і штраф – 3 рази. 16 осіб звільнені від відбування покарання з випробуванням, 1 особа звільнена з інших підстав.

Щодо *третьої групи* кримінальних правопорушень проти інформаційної безпеки, то вона включає п'ять статей та дев'ять кримінальних правопорушень і санкцій за ці правопорушення[1]. З них 1 (11,1%) – за проступок, 6 (66,7%) – це нетяжкі злочини, 2 (22,2%) – тяжкі злочини. Шість санкцій – альтернативні, а 3 – безальтернативні.

Позбавлення волі міститься у 8, обмеження волі – у 3, арешт – у 3, виправні роботи – у 3, позбавлення права обіймати певні посади або займатися певною діяльністю – у 1. Всі санкції є відносновизначеними. П'ять санкцій містять конфіскацію майна як додаткове покарання, яке суд може застосувати або ні (кумулятивні санкції з альтернативним покаранням). Одна передбачає позбавлення права обіймати певні посади або займатися певною діяльністю як безальтернативне додаткове покарання.

Щодо практики застосування покарання за 2021 та 2022 рр. можна зазначити таке. У 2021 р. за вказані кримінальні правопорушення було засуджено 14 осіб, а у 2022 р. – 373 осіб. У 2021 р. – п'ятьом особам призначений штраф, 9 осіб – звільнені від відбування покарання з випробуванням.

У 2022 р. довічне позбавлення волі застосовувалось 1 раз, позбавлення волі призначалося 23 рази, у тому числі у розмірах 1 рік – 2, понад 1 рік до 2 років включно – 4, понад 2 роки до 3 років включно – 11, понад 3 роки до 5 років включно – 5, понад 5 років до 10 ро-

[1] При аналізі не досліджувалося посягання на територіальну цілісність і недоторканність України, у зв'язку з тим, що неможливо окремо виокремити правопорушення проти інформаційної безпеки.

ків включно – 1, обмеження волі – 3, арешт – 4, виправні роботи – 3, громадські роботи – 1, позбавлення права обіймати певні посади або займатися певною діяльністю – 133, і штраф – 10 разів, інші види – 1. 208 осіб звільнені від відбування покарання з випробуванням. Додаткове покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю призначалося 1 раз, конфіскація майна – 4 рази.

Отже, кримінальні правопорушення проти інформаційної безпеки сумарно містяться в 17 статтях чинного КК України, які включають в себе 37 складів кримінальних правопорушень. Серед яких: 5 проступків (13,5%), 20 нетяжких злочинів (54,1%), 8 тяжких (21,6%) і 4 особливо тяжких (10,8%). У 8 санкціях міститься штраф (21,6%)[1], в 1 – позбавлення права обіймати певні посади або займатися певною діяльністю (2,7%), в 5 – виправні роботи (13,5%), в 3 – арешт (8,1%), в 10 – обмеження волі (27%) і в 32 – позбавлення волі (86,5%).

Проведене дослідження дозволило зробити такі висновки:

1. Кримінальні правопорушення проти інформаційної безпеки можна умовно поділити на три групи: кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361, 361[1], 361[2], 362, 363, 363[1] КК України); кримінальні правопорушення, що посягають на суспільні відносини у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави (ст.ст. 111 – в частині шпигунства, 114, 114[2], 328, 329, 330 – в частині інформації зібраної у процесі контррозвідувальної діяльності та у сфері оборони країни, та 422 КК України); кримінальні правопорушення спрямовані на інформаційний простір держави (ст.ст. 109 – в частині публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, 110 – в частині публічних закликів чи роз-

[1] Новікова К.А. Питання караності кримінальних правопорушень проти інформаційної безпеки держави за кримінальним законодавством України. *Питання боротьби зі злочинністю* : зб. наук. пр. / редкол.: В. С. Батиргареєва (голов. ред.) та ін. Харків : Право, 2023. Вип. 46. С. 41-47.

повсюдження матеріалів із закликами до зміни меж території або державного кордону України, 111[1] (ч. 1, ч. 3 та ч. 6 – в частині здійснення інформаційної діяльності у співпраці з державою-агресором), 436, 436[1] та 436[2] КК України).

2. Кримінальні правопорушення проти інформаційної безпеки сумарно містяться в 17 статтях чинного КК України, які включають в себе 37 складів кримінальних правопорушень, серед яких: 5 проступків (13,5%), 20 нетяжких злочинів (54,1%), 8 тяжких (21,6%) і 4 особливо тяжких (10,8%). Отже, переважно кримінальні правопорушення проти інформаційної безпеки є нетяжкими або тяжкими злочинами.

3. У санкціях цих правопорушень переважають позбавлення волі (86%), обмеження волі (27%), штраф (21,6%).

Висновки

1. Встановлено, що державна політика у сфері кримінально-правового забезпечення інформаційної безпеки має тісний зв'язок з міжнародними та європейськими стандартами з прав людини, що визначені передусім положеннями ЄКПЛ та практикою ЄСПЛ, і, зокрема, законами та звичаями війни (що прямо або опосередковано відповідають нормативним положенням КК України).

2. Показано зв'язок між чинним кримінальним законодавством та стратегіями, концепціями і програмами, що прийняті в Україні з метою забезпечення інформаційної безпеки та кібербезпеки в державі.

3. Зазначено, що в умовах спротиву широкомасштабній російській агресії проти України політика нашої держави у сфері кримінально-правового забезпечення інформаційної безпеки сконцентрована на протидії ворожим кібератакам, деструктивній пропаганді, дезінформації та іншим проявам інформаційних загроз.

4. Підкреслена важлива роль Стратегії інформаційної безпеки України 2021 р. та Стратегії кібербезпеки України 2021 р. для кримінально-правової політики, в яких визначені цілі й завдання протидії державі-агресору та її атакам у площині не тільки забезпечення ін-

формаційної безпеки та кібербезпеки, а й суверенітету (зокрема, й інформаційного) та незалежності України. Зауважено, що на відміну від положень законодавства України про кримінальну відповідальність, приписи вищеозначених документів орієнтують державні органи на виконання конкретних заходів, реалізація яких прямо пов'язується з певними стратегічними цілями, визначеними в цих документах, і які фактично являють собою своєрідну дорожню карту.

5. Зазначено, що під час війни для кримінально-правового забезпечення інформаційної безпеки набувають першочергового значення норми Особливої частини КК, що мають об'єктом охорони інформаційну безпеку або ж мають в системі ознак кримінального правопорушення інформацію як предмет (знаряддя, засіб), що використовується для вчинення суспільно небезпечного діяння. Кримінальні правопорушення, що передбачені такими нормами поділені на групи:1) злочини проти основ національної безпеки; 2) кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; 3) інші кримінальні правопорушення у сфері охорони державної таємниці та іншої інформації, що забезпечують обороноздатність держави; 4) кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку.

6. Інформаційний суверенітет є невід'ємною ознакою сучасної держави і водночас юридичним механізмом формування та реалізації внутрішньої та зовнішньої інформаційної політики держави, обумовленої національними інтересами України в цій сфері, та спрямованої, здебільшого, на забезпечення інформаційної безпеки як складової національної безпеки України.

7. Установлено, що у кримінально-правовій охороні інформаційної безпеки дітей можливо виділити загальний, спеціальний, особливий та окремий рівні за критерієм їх конкретизованості. При цьому така охорона виражається в сукупності кримінально-правових норм, в яких закріплено відповідальність за посягання на життя та здоров'я дітей, їх волю, честь та гідність, власність, нормальний розвиток від негативного інформаційного впливу, інших операцій із ін-

формацією, незаконного використання інформаційно-комунікаційних систем, а також незаконних дій інших осіб із інформацією з обмеженим доступом.

Виявлено, що протягом останніх шести років намітилася тенденція посилення кримінально-правової охорони інформаційної безпеки дітей у виді запровадження відповідальності за певні суспільно небезпечні прояви шляхом введення до КК України нових норм або ж внесення змін до чинних його норм.

8. Вивчення караності правопорушень проти інформаційної безпеки дало змогу виділити та диференціювати за видами загальну кількість кримінально-правових санкцій, що можуть бути застосовані до осіб, винних у вчинені зазначених правопорушень, і констатувати, що в абсолютній більшості випадків основним видом покарання для них буде позбавлення волі на певний строк, що відповідає ступеню тяжкості таких кримінальних правопорушень.

Авторський колектив

РОЗДІЛ 1

М. В. КАРЧЕВСЬКИЙ — д-р юрид. наук, проф., гол. наук. співроб. Інституту (вступ; підрозд. 1.1; 1.2 у співавт. з Н. В. Шульженко; 1.4; висновки)

Н. В. ШУЛЬЖЕНКО — канд. юрид. наук, доц., ст. наук. співроб. Інституту (підрозд. 1.2 у співавт. з М. В. Карчевським; висновки)

Д. О. КУКОВИНЕЦЬ — мол. наук. співроб. Інституту (підрозд. 1.3; висновки)

РОЗДІЛ 2

М. В. ШЕПІТЬКО — д-р юрид. наук, проф., пров. наук. співроб. Інституту (вступ; підрозд. 2.1 у співавт. з В. І. Борисовим; висновки)

В. І. БОРИСОВ — акад. НАПрН України, д-р юрид. наук, проф., радник при дирекції Інституту (підрозд. 2.1 у співавт. з М. В. Шепітьком; висновки)

В. В. БАЗЕЛЮК — канд. юрид. наук, доц., мол. наук. співроб. Інституту (підрозд. 2.2)

В. В. ФЕДЮК — мол. наук. співроб. Інституту (підрозд. 2.3)

Д. П. ЄВТЄЄВА — канд. юрид. наук, ст. дослідник, заст. директора з наук. роботи Інституту (підрозд. 2.4)

К. А. НОВІКОВА — канд. юрид. наук, ст. наук. співроб. Інституту (підрозд. 2.5)

Д. О. КУКОВИНЕЦЬ — мол. наук. співроб. Інституту (висновки)

Наукове видання

Борисов Вячеслав Іванович,
Карчевський Микола Віталійович,
Шепітько Михайло Валерійович та ін.

МІЖНАРОДНІ СТАНДАРТИ ТА НАЦІОНАЛЬНА КРИМІНАЛЬНО-ПРАВОВА ПОЛІТИКА У СФЕРІ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Монографія

Електронне наукове видання

Комп'ютерна верстка *А. Т. Гринченка*

Підписано до поширення через мережу Інтернет 29.12.2023.
Відповідає формату друкованого видання 60×84/16. Гарнітура Times.
Обл.-вид. арк. 7. Об'єм даних 2,5 Мб.
Вид. № 3281

Видавництво «Право» Національної академії правових наук України та
Національного юридичного університету імені Ярослава Мудрого,
вул. Чернишевська, 80, Харків, 61002, Україна
E-mail для авторів: verstka@pravo-izdat.com.ua
E-mail для замовлень: sales@pravo-izdat.com.ua
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої
продукції – серія ДК № 4219 від 01.12.2011