УДК343.3/.7
DOI: https://doi.org/10.33216/2218-5461/2024-47-1-120-129

ОСНОВНІ ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ[1]

Карчевський М.

THE MAIN PROBLEMS OF CRIMINAL-LEGAL PROTECTION OF INFORMATION SECURITY IN UKRAINE

Karchevskyi M.

Досліджуються проблеми кримінально-правової охорони елементів інформаційної безпеки. Інформаційна безпека визначається як сукупність суспільних відносин, в межах яких забезпечується реалізація інформаційних потреб громадян, суспільства держави. Ця система 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 його діяльність забезпечена повною, правдивою та достатньою для прийняття рішень інформацією.

До проблем інформаційної безпеки у сфері використання інформаційних технологій віднесені: примітивізація протидії кримінальним правопорушенням; неготовність протидії злочинному використанню віртуальних активів; слабкість протидії злочинному використанню технологій штучного інтелекту й неповноцінна робота щодо використання нових технологій для протидії злочинності.

Проблемою кримінально-правової охорони інформаційної безпеки у сфері забезпечення доступу до інформації визначено надмірну кількість кримінально-правових заборон.

Ключова проблема кримінально-правової охорони інформаційної безпеки у сфері формування інформаційного ресурсу полягає у чіткому визначенні меж ефективного кримінально-правового впливу.

В умовах, коли війна рф проти нашої країни має більше ніж значну інформаційну складову, існування означених проблем кримінально-правового регулювання у сфері інформаційної безпеки створює додаткові небезпеки та потребує якнайшвидшого реагування.

Ключові слова: *кримінальне право, ефективність протидії кримінальним правопорушенням, інформаційна безпека*

Постановка проблеми. Війна рф проти України ставить підвищені вимоги до правового регулювання. Протидія агресору вимагає ефективного використання всіх наявних ресурсів. Більше ніж значна частина агресії відбувається в інформаційному просторі. Кримінальне право, як ultima ratio, фокусується на найбільш небезпечних посяганнях. Воно використовує найбільш суворі засоби реагування на винних осіб та,

[1] Статтю підготовлено в межах фундаментальної теми «Теоретичні, законодавчі та правозастосовні проблеми кримінально-правової охорони інформаційної безпеки в Україні» (номер державної реєстрації 0121U114324).

відповідно, потребує значних соціальних ресурсів для реалізації. Названі чинники зумовлюють необхідність аналізу ефективності кримінально-правової охорони інформаційної безпеки в Україні.

Стан дослідження. Інформаційна безпека розглядалася в межах багатьох контекстів соціальної науки. Вона була предметом досліджень у сфері теорії права [7], основ національної безпеки [8;9], адміністративного права [10;11;12], політології [13], міжнародних відносин [14] тощо. Зрозуміло, що предметне поле певної наукової галузі визначає особливості змісту інформаційної безпеки. Для кримінально-правового виміру проблеми так специфіка визначається наступним чином.

По-перше, розглядається як система суспільних відносин, а не певний стан або захищеність. Саме суспільні відносини є предметом правового регулювання, це аксіома. Право регулює не стани, а відносини.

По-друге, кримінально-правове регулювання інформаційної безпеки відбувається за допомогою норм, що передбачають посягання на різноманітні родові об'єкти. Це відбувається тому, що норми, які регулюють отримання, передачу, поширення або захист інформації присутні у великій кількості регулятивних галузей права.

По-третє, для визначення інформаційної безпеки в межах кримінально-правового регулювання необхідним є встановлення соціальних потреб, які зумовлюють необхідність кримінально-правової охорони. Йдеться про інформаційну потребу, яка є чинником появи та функціонування суспільних відносин інформаційної безпеки [15,с.8].

Отже, інформаційна безпека розуміється нами як система суспільних відносин, що забезпечує можливість реалізації інформаційної потреби громадян, суспільства, держави. Інформаційна потреба реалізується, коли отримано доступ до необхідної інформації. Технічною базою реалізації інформаційної потреби є використання інформаційних технологій. Формування інформаційного ресурсу забезпечує реалізацію інформаційної потреби. Таким чином, 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» [15,с.9].

Про перебування суб'єкта в стані інформаційної безпеки ми говоримо тоді, коли прийняття ним рішень забезпечено інформацією, яка достатньо повно характеризує предмет діяльності, є правдивою та достатньою для прийняття ефективних рішень. Елементами інформаційної безпеки є суспільні відносини: у сфері використання інформаційних технологій, у сфері забезпечення доступу до інформаційного ресурсу й у сфері формування інформаційного простору. «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. Серед означених суспільних відносин ті, які охороняються законом про кримінальну відповідальність, і складають зміст інформаційної безпеки як об'єкта кримінально-правової охорони» [15,с.9].

Систематизуємо проблеми кримінально-правової охорони інформаційної безпеки з урахуванням визначених елементів. Для використання інформаційних технологій це примітивізація та неготовність до використання злочинцями новітніх

технологій, в першу чергу віртуальних активів та штучного інтелекту. Проблемою кримінально-правової охорони відносин інформаційної безпеки у сфері забезпечення доступу до інформації є надмірна розгалуженість та розбалансованість заборон. Визначення меж використання засобів кримінально-правового впливу є основною проблемою для відносин у сфері формування інформаційного простору.

Метою статті є: аналіз названих проблем кримінально-правової охорони інформаційної безпеки в Україні.

Виклад основного матеріалу: Дані офіційної статистики за останні одинадцять років (2013-2023) свідчать про те, що кількість проваджень, облікованих за ознаками кримінальних правопорушень, передбачених Розділом XVI Особливої частини КК, зросла від половини тисячі до майже чотирьох тисяч на рік, тоді як кількість засуджених осіб змінилася від 72 до 126 на рік (рис. 1). Реальні покарання у випадках засудження за ці кримінальні правопорушення застосовувалися у 50% випадків (середній показник для всіх випадків засудження – 58%). Як правило за «комп'ютерні» кримінальні правопорушення суди призначали штраф (75%). Позбавлення волі призначалося кожному п'ятому засудженому (21%). Порівняння цих показників із практикою призначення покарань в означений період за всі кримінальні правопорушення також свідчить, що до «комп'ютерних» злочинців судді ставилися більш поблажливо. За період з 2013 по 2023 серед засуджених за всі кримінальні правопорушення, штраф було призначено 39%, позбавлення волі – 36%.

Таким чином кримінально-правовий вплив на осіб, що вчинили «комп'ютерні» кримінальні правопорушення (ст.ст. 361 – 363-1 КК) є менш інтенсивним, характеризується рідшим застосуванням реальних покарань та частішим використан-

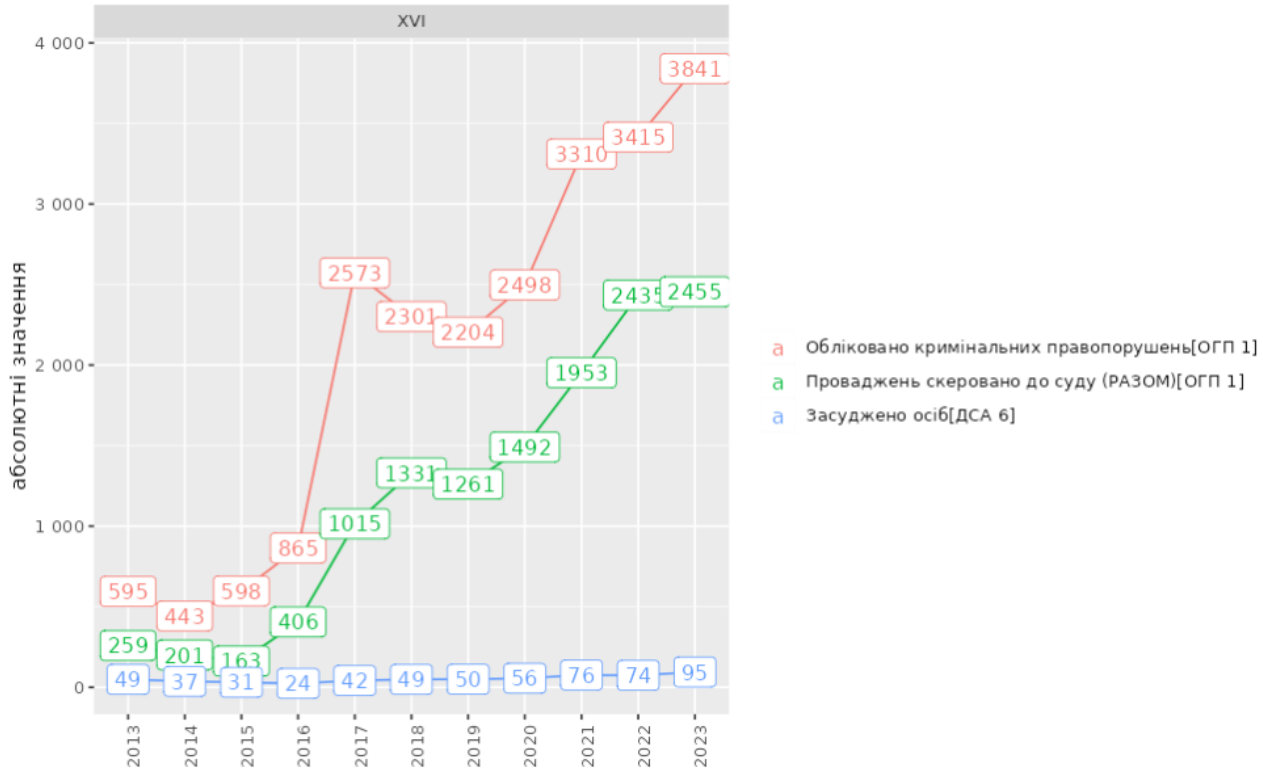

Рис. 1.

ням більш м'яких покарань. Все це відбувається в умовах подальшого розширення сфери застосування інформаційних технологій та, відповідно, збільшення уразливості суспільних відносин від посягань у вигляді «зламів» інформаційних систем, так званих атак відмов від обслуговування тощо. Вважаємо, що це може свідчити про те, що у поле зору кримінальної юстиції потрапляють переважно найпростіші та найменш небезпечні форми відповідних кримінальних правопорушень [4]. Таку проблему ми називаємо примітивізацією правозастосовчого рівня кримінально-правового регулювання. Вона не є новою. За результатами дослідження судової практики по Розділу XVI Особливої частини КК ще у 2012 році ми зробили наступний 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, більш ніж половина судових рішень досліджуваної категорії (56,29%) пов'язані з кваліфікацією таких діянь, віднесення яких до суспільно небезпечних є досить спірним [6,с.221]. Впевнені, що аналогічна проблема існує і зараз. Для її виявлення достатньо провести контент-аналіз вироків відповідної категорії, представлених у Єдиному державному реєстрі судових рішень.

У цьому контексті не можна не звернути уваги на Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24.03.2022 № 2149-IX. Закон передбачав зміни до Розділу XVI. Зокрема здійснено самостійну криміналізацію несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ч.1 ст. 361). Дії які раніше вважалися основним складом кримінального правопорушення передбаченого цією нормою стали його особливо кваліфікованим складом (ч.3 ст. 361) і отримали більш сувору санкцію. В умовах встановлених тенденцій примітивізації протидії «комп'ютерним» кримінальним правопорушенням, названі зміни законодавства про кримінальну відповідальність мають негативний потенціал. Вони можуть стати причиною появи у сфері дії кримінальної юстиції ще більшої кількості діянь, які характеризуються спірною суспільною небезпечністю та не потребують заходів кримінально-правового впливу.

Позначена раніше проблема тисяч матеріалів, надісланих до національних судів з обвинуваченням осіб у вчиненні кримінальних правопорушень, передбачених Розділом XVI Особливої частини КК, та близько однієї сотні засуджених (рис. 1), може бути частково пояснена особливостями статистичного обліку, який здійснює Державна судова адміністрація України (ДСА). Судові рішення фіксуються у звітах за найтяжчим обвинуваченням. Можливо звинувачення в незаконних діях з інформаційними технологіями у переважній більшості супроводжуються звинуваченнями в більш серйозних злочинах (шахрайство, вимагання тощо). Тому в статистичних звітах Офісу Генерального Прокурора відповідні обвинувальні матеріали фіксуються, а у звітах ДСА – ні. Така гіпотеза потребує подальшої перевірки, але якщо вона підтвердиться, цілком слушним буде провокаційне, але лише на перший погляд, питання: «Може, настав час замислитися, чи існують насправді «комп'ютерні» злочини?». Якщо переважна більшість випадків супроводжується звинуваченням у вчиненні більш тяжких кримінальних правопорушень, якщо

«самостійні» звинувачення характеризуються переважно звільненням від покарання та застосуванням штрафів, чи не буде правильним розглядати «комп'ютерні» кримінальні правопорушення просто як спосіб старої, добре відомої крадіжки або вимагання чи шахрайства? Зрозуміло порушені питання потребують самостійного дослідження, однак їх актуальність є значною, особливо в контексті проблеми ефективного використання соціальних ресурсів для протидії злочинності.

Наступна проблема, готовність до використання віртуальних активів для вчинення кримінальних правопорушень. Головний аспект у даному питанні - незавершеність правового регулювання використання віртуальних активів на національному рівні (прийнято відповідний закон, але він набере чинності після внесення змін до Податкового кодексу). За умови, що «розмітку» правового поля не завершено, відбувається фактичне використання віртуальних активів для вчинення кримінальних правопорушень.

Існує певний вакуум щодо визначеності дій правоохоронців у випадку вилучення віртуальних активів, визначення їх вартості в національній валюті, збереження після вилучення тощо. Організаційно-технічне забезпечення вказаних процесів за нашою оцінкою є недостатнім. Тому факти злочинного використання криптовалюти з великою ймовірністю не отримують належного реагування. Наприклад, вилучення криптовалюти доцільно організовувати як транзакцію на електронний гаманець, що контролюється правоохоронним органом. Водночас порядок створення таких гаманців, документування цього процесу дотепер не отримали нормативного регулювання.

Міжнародні експерти зазначають, що розширення сфери застосування віртуальних активів меншою мірою потребує змін кримінального законодавства, але актуалізує завдання правового регулювання обігу віртуальних активів на національному рівні[2]. Це справедливо і для України.

Істотні зміни «комп'ютерної» злочинності пов'язують з розповсюдженням технологій *штучного інтелекту* [3]. Обґрунтованим є прогноз їх широкого використання для злочинних цілей [1]. Сучасна міжнародна дискусія щодо правового регулювання соціалізації штучного інтелекту характеризується більшою увагою до практичних та прикладних 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. В першу чергу, для обмеження сфери нормативного впливу та структурування національного юридичного та технічного дискурсів, необхідне нормативне визначення систем штучного інтелекту. Далі, наслідуючи європейський підхід, доцільним буде здійснення класифікації систем штучного інтелекту за ступенем ризику, формулювання для кожного виду пропорційних можливим небезпекам нормативних вимог до розробки та використання. Регулювання використання систем ШІ національними правоохоронними має відбуватися у спосіб формулювання спеціальних норм до загальних правил, які названі вище. Водночас використання технологій ШІ національними правоохоронними органами без чітких та зрозумілих законодавчих положень про можливі обмеження приватності громадян, створює реальну небезпеку визнання діяльності правоохоронців незаконною навіть за формальною ознакою (не «відповідно до закону») [3].

Основна проблема кримінально-правової охорони відносин інформаційної безпеки у сфері забезпечення доступу до інформації полягає у надмірній кількості кримінально-правових заборон у даній сфері. Предметом значної кількості кримінальних правопорушень, передбачених чинним КК, є інформація з обмеженим доступом, об'єктивна сторона таких посягань полягає у різноманітних формах порушення обмеженого доступу до такої інформації. До таких кримінальних правопорушень можна віднести: державну зраду (ст. 111); шпигунство (ст. 114); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132); незаконне розголошення лікарської таємниці (ст. 145); порушення таємниці голосування (ст. 159); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163); розголошення таємниці усиновлення (удочеріння) (ст. 168); порушення недоторканності приватного життя (ст. 182); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231); розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках (ст. 232); незаконне використання інсайдерської інформації (ст. 233); розголошення державної таємниці (ст. 328); 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) тощо.

Існування такої кількості окремих норм для різних видів інформації з обмеженим доступом є невиправданим і таким, що потребує оптимізації. Способом розв'язання даної проблеми може стати заміна наявних у КК спеціальних заборон однією спеціальною. Інтенсивність покарання в такому випадку доцільно визначати не за видом інформації з обмеженим доступом, а за спричиненою шкодою. Наприклад, цілком очевидно, що шкода навіть від розголошення відомостей, що складають державну таємницю, далеко не завжди є значно більшою ніж шкода від розголошення таємниці усиновлення або удочеріння.

Основним питанням кримінально-правової охорони відносин у сфері формування інформаційного простору є визначення меж та оцінка ефективності заходів кримінально-правового впливу. Ризики й небезпеки інформаційних впливів широко обговорюються у юридичному дискурсі. Не викликає сумнівів небезпечність інформаційного простору позбавленого правового регулювання. Разом з цим, традиційне доповнення КК новими заборонами тут видається найменш ефективним. Глобалізація інформаційних процесів та добре відомий «ефект Стрейзанд» найкраще підтверджують цю тезу [15,с.16].

Розширення засобів кримінально-правової охорони в інформаційній сфері обов'язково має враховувати соціально негативний вплив заборон. Коли мінімізація ризиків використання інформаційних технологій можлива шляхом застосування інших, не кримінально-правових інструментів, доцільно використовувати саме їх. У складі команди з реалізації проєкту «Кримінально-правові та кримінологічні засади протидії глорифікації збройної агресії рф в Україні» (реєстраційний номер 2022.01/0060), що виконується за підтримки Національного фонду досліджень України, ми здійснили комплексне дослідження питань відповідальності за глорифікацію дій ворога

(ст. 436-2 КК). Було встановлено невідповідність цілей та прогнозів соціальних ефектів криміналізації. Суди у переважній більшості розглядали справи наймеш небезпечних проявів виправдовування ворога («лайки» у соціальних медіа). За умови активних дій противника в інформаційній сфері, такий прояв примітивізації кримінально-правового регулювання є небезпечним. Навряд чи така сукупність судових рішень забезпечує досягнення задекларованих цілей криміналізації виправдовування дій агресора [4].

Подальша практика протидії переважно менш небезпечним формам глорифікації приведе до спрощеного розуміння глорифікації у публічному соціально-політичному дискурсу. Своєю чергою, «девальвація небезпеки» спростить використання глорифікації агресором для досягнення військових цілей. Цього не можна допускати. Необхідним є фокусування протидії на дійсно небезпечних проявах глорифікації (адміністрація каналів соціальних медіа, створення та підтримання мереж та званих «ботів» тощо). Також є сенс використовувати позитивний інформаційний вплив, більш активно використовувати суспільну комунікацію, інформувати громадськість про небезпеки глорифікації та ефективні дії правоохоронців.

Висновки. Розгляд інформаційної безпеки як об'єкта кримінально-правової охорони та визначення її в цьому контексті як сукупності суспільних відносин в межах яких забезпечується реалізація інформаційних потреб громадян, суспільства держави, є методологічно послідовним та дозволяє якісно організувати науковий аналіз проблем кримінально-правової охорони інформаційної безпеки.

До проблем інформаційної безпеки у сфері використання інформаційних технологій віднесені: примітивізація протидії кримінальним правопорушенням; неготовність протидії злочинному використанню віртуальних активів; слабкість протидії злочинному використанню технологій штучного інтелекту й неповноцінна робота щодо використання нових технологій для протидії злочинності.

Проблемою кримінально-правової охорони інформаційної безпеки у сфері забезпечення доступу до інформації є надмірна кількість кримінально-правових заборон, є потреба оптимізації.

Ключова проблема кримінально-правової охорони інформаційної безпеки у сфері формування інформаційного ресурсу полягає у необхідності чіткого визначення меж ефективного кримінально-правового впливу.

В умовах, коли війна рф проти нашої країни має більше ніж значну інформаційну складову, існування означених проблем кримінально-правового регулювання у сфері інформаційної безпеки створює додаткові небезпеки та потребує якнайшвидшого реагування.

Література:

1. Dupont B., Stevens Y., Westermann H., Joyce M. Artificial Intelligence in the Context of Crime and Criminal Justice. Korean Institute of Criminology. Canada : Université de Montréal, 2019. P. 33-37. URL: https://www.researchgate.net/publication/337402608_Artificial_Intelligence_in_the_Context_of_Crime_and_Criminal_Justice (дата звернення: 09.05.2024).

2. Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering. 6th Global Conference on *Criminal Finances and Cryptocurrencies* on 1–2 September 2022. URL: https://baselgovernance.org/publications/seizing-opportunity-5-recommendations-crypto-assets-related-crime-and-money-laundering (дата звернення: 12.05.2024).

3. Карчевський М.В., Куковинець Д.О. Використання технологій штучного інтелекту

правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*: зб. наук. пр. / редкол.: В.С. Батиргареєва (голов. ред.) та ін. Харків : Право. 2023. Вип. 46. С. 21-31.

4. Карчевський М.В. Протидія виправдовуванню, визнанню правомірною, запереченню збройної агресії російської федерації проти України, глорифікації її учасників: очікування та реальність. *Законодавчі аспекти протидії особливо небезпечним злочинам в Україні*. Матеріали міжнародного науково-практичного круглого столу 14-15 березня 2024 року, м. Київ. Київ : Алерта, 2024. С. 122–126. URL: https://dspace.nlu.edu.ua/bitstream/123456789/20022/1/ZAPONZU.pdf (дата звернення: 19.05.2024).

5. Карчевський М.В. Протидія кримінальним правопорушенням у сфері використання інформаційних технологій в Україні. *Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану.* Матеріали міжнародної науково-практичної конференції м. Чернігів, 25–26 квітня 2023 року: у двох томах / голов. ред. В. Ф. Пузирний. Чернігів : Академія ДПтС, 2023. С. 125-131. URL: https://academysps.edu.ua/wp-content/uploads/2023/06/Konferenciya-Tom-1-_25-26-kvitnya_2023.pdf (дата звернення: 07.05.2024).

6. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.

7. Тихомиров О.О. Забезпечення інформаційної безпеки як функція держави : автореф. дис. ... кандидата юрид. наук : 12.00.01. К., 2011. 19 с.

8. Горбулін В.П. Биченок М.М. Проблеми захисту інформаційного простору України : монографія; Інститут проблем національної безпеки. К. : Інтертехнологія. 2009. 136 с.

9. 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.

10. Кормич Б.А. Інформаційна безпека: організаційно правові основи : навч. посібник. К. : Кондор, 2004. 384 с.

11. Марущак А.І. Інформаційне право: доступ до інформації : навч. посіб. для студ. ВНЗ. К. : КНТ, 2007. 531 с.

12. Ліпкан В.А. Адміністративно-правові основи забезпечення національної безпеки України : автореф. дис… доктора юрид. наук : 12.00.07. К., 2008. 34 с.

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

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

15. Міжнародні стандарти та національна кримінально-правова політика 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. URL: https://ivpz.kh.ua/wp-content/uploads/2024/03/%D0%9C%D0%BE%D0%BD%D0%BE_%D0%86%D0%BD%D1%84%D0%BE%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_2023_%D0%9D%D0%94%D0%86-%D0%92%D0%9F%D0%97_%D0%B0%D0%B2%D1%82_compressed.pdf (дата звернення: 17.05.2024).

References:

1. Dupont B., Stevens Y., Westermann H., Joyce M. (2019). Artificial Intelligence in the Context of Crime and Criminal Justice. Korean Institute of Criminology. Canada : Université de Montréal. P. 33-37 (in English).

2. Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering. (2022). *6th Global Conference on Criminal Finances and Cryptocurrencies* on 1–2 September (in English).

3. Karchevskyi, M.V., Kukovynets, D.O. (2023). Vykorystannia tekhnolohii shtuchnoho intelektu pravookhoronnymy ta sudovymy orhanamy:

svitovyi dosvid ta napriamy rozvytku natsionalnoho zakonodavstva. *Pytannia borotby zi zlochynnistiu*: zb. nauk. pr. / redkol.: V.S. Batyrhareieva (holov. red.) ta in. Kharkiv : Pravo. Vyp. 46. S. 21-31 (in Ukrainian).

4. Karchevskyi, M.V. (2024). Protydiia vypravdovuvanniu, vyznanniu pravomirnoiu, zaperechenniu zbroinoi ahresii rosiiskoi federatsii proty Ukrainy, hloryfikatsii yii uchasnykiv: ochikuvannia ta realnist. *Zakonodavchi aspekty protydii osoblyvo nebezpechnym zlochynam v Ukraini*. Materialy mizhnarodnoho naukovo-praktychnoho kruhloho stolu 14-15 bereznia 2024 roku, m. Kyiv. Kyiv : Alerta. S. 122–126 (in Ukrainian).

5. Karchevskyi, M.V. (2023). Protydiia kryminalnym pravoporushenniam u sferi vykorystannia informatsiinykh tekhnolohii v Ukraini. *Aktualni pytannia teorii ta praktyky v haluzi prava, osvity, sotsialno-humanitarnykh ta povedinkovykh nauk v umovakh voiennoho stanu*. Materialy mizhnarodnoi naukovo-praktychnoi konferentsii m. Chernihiv, 25–26 kvitnia 2023 roku: u dvokh tomakh / holov. red. V. F. Puzyrnyi. Chernihiv : Akademiia DPtS. S. 125-131 (in Ukrainian).

6. Karchevskyi, M.V. (2012). Kryminalno-pravova okhorona informatsiinoi bezpeky Ukrainy : monohrafiia. Luhansk : RVV LDUVS im. E. O. Didorenka. 528 s. (in Ukrainian).

7. Tykhomyrov, O.O. (2011). Zabezpechennia informatsiinoi bezpeky yak funktsiia derzhavy : avtoref. dys. ... kandydata yuryd. nauk : 12.00.01. 19 s. (in Ukrainian).

8. Horbulin, V.P., Bychenok M.M. (2009). Problemy zakhystu informatsiinoho prostoru Ukrainy : monohrafiia; Instytut problem natsionalnoi bezpeky. K. : Intertekhnolohiia. 136 s. (in Ukrainian).

9. Konakh, V.K. (2005). Zabezpechennia informatsiinoi bezpeky derzhavy yak skladovoi systemy natsionalnoi bezpeky (pryklad SShA) : avtoref. dys. … kandydata polit. nauk: 21.01.01. K. 20 s. (in Ukrainian).

10. Kormych, B.A. (2004). Informatsiina bezpeka: orhanizatsiino pravovi osnovy: navch. posibnyk. K. : Kondor. 384 s. (in Ukrainian).

11. Marushchak, A.I. (2007). Informatsiine pravo: dostup do informatsii: navch. posib. dlia stud. VNZ. K. : KNT. 531 s. (in Ukrainian).

12. Lipkan, V.A. (2008). Administratyvno-pravovi osnovy zabezpechennia natsionalnoi bezpeky Ukrainy : avtoref. dys… doktora yuryd. nauk: 12.00.07. K. 34 s.

13. Sashchuk, H.M. (2005). Bezpekovi imperatyvy televiziinoho prostoru Ukrainy: avtoref. dys. … kandydata polit.nauk: 23.00.03. K. 16 s. (in Ukrainian).

14. Skliarenko, O.A. (2006). Suchasni problemy informatsiinoi bezpeky Ukrainy v umovakh vnutrishnikh transformatsii. *Aktualni problemy mizhnarodnykh vidnosyn*. Vypusk 64 (Chastyna I). S. 125–131 (in Ukrainian).

15. Mizhnarodni standarty ta natsionalna kryminalno-pravova polityka u sferi okhorony informatsiinoi bezpeky: monohrafiia : elektron. nauk. vyd. / za zah. red. V. I. Borysova, M. V. Karchevskoho, M. V. Shepitka ; Nats. akad. prav. nauk Ukrainy ; NDI vyvch. problem zlochynnosti im. akad. V. V. Stashysa NAPrN Ukrainy. Kharkiv : Pravo, 2023. 152 s. (in Ukrainian).

Karchevskyi M. The main problems of criminal-legal protection of information security in Ukraine - Article.

Problems of criminal protection of elements of information security are determined. Information security is defined as a set of social relations within which the information needs of citizens, society and the state are realized. This system includes: 1) relations to ensure access to information resources; 2) relations regarding the formation of an information resource; 3) relations regarding ensuring the functioning of information technologies as a means of access to the information resource and its formation.

The entity is in a state of information security when its activities are provided with complete, reliable and sufficient information for decision-making.

The problems of information security in the field of the use of information technologies include: primitiveization of combating criminal offenses; unpreparedness to combat the criminal use of virtual assets; unpreparedness for the criminal use of artificial intelligence technologies and unpreparedness for their full use to combat crime.

The problem of criminal law protection of information security in the field of ensuring access to information is defined as an excessive number of criminal law prohibitions.

The key problem of criminal law protection of information security in the field of information resource formation is the clear definition of the limits of effective criminal law influence.

In the conditions when the war of the Russian Federation against our country has more than a significant informational component, the existence of certain problems of criminal law regulation in the field of information security creates additional dangers and requires the fastest possible response.

Keywords: *criminal law, effectiveness of combating criminal offenses, information security*

Авторська довідка.

Карчевський Микола Віталійович *– доктор юридичних наук, професор, професор кафедри кримінального права і кримінології Львівського державного університету внутрішніх справ, головний науковий співробітник відділу дослідження проблем кримінального права Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України. ORCID: https://orcid.org/0000-0002-2693-3592*

Стаття надійшла до редакції 18 квітня 2024р.