Інформаційна і національна безпека

УДК 343.2

БАРАНОВ. О.А., *доктор юридичних наук, професор*,
керівник наукового центру ДНУ ІБП НАПрН України.
ORCID: https://orcid.org/0000-0003-3233-6687.

ШЛЯХИ ВДОСКОНАЛЕННЯ ПРАВОВОЇ БАЗИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Анотація. *Процеси тотальної цифровізації характеризуються разючими позитивними результатами, які вони привносять у суспільство. Водночас цифровізація стає джерелом певних загроз, серед яких особливе місце посідають проблеми кіберзлочинності. На рівні світової спільноти та окремих держав докладається багато зусиль щодо формування ефективної правової бази боротьби з цим постійно зростаючим, загрозливим явищем. Але результати поки що є невтішними, причиною є недостатність розуміння "туманної природи" кіберзлочинних діянь.*

У статті з'ясовуються глибинні причини та механізми негативного впливу кіберзлочинності на життя суспільства та на життя окремої людини. Обґрунтовується тісний діалектичний взаємозв'язок між кіберзлочинністю та інформаційною та кібербезпекою. Розкривається зміст та умови забезпечення інформаційної та кібербезпеки. Стверджується, що навмисне чи ненавмисне порушення цих умов становить зміст родового об'єкта кіберзлочину. Для вирішення певних проблем у галузі кримінального права, пов'язаних із цифровими технологіями, запропоновано проведення конкретних досліджень.

Ключові слова*: інформаційна безпека, кібербезпека, кіберзлочин, цифрові технології, кодекс.*

Summary. *The processes of total digitalization are characterized by striking positive results that they bring to society. At the same time, digitalization becomes a source of certain threats, among which the problems of cybercrime occupy a special place. At the level of the world community and individual states, many efforts are being made to create an effective legal framework for combating this ever-growing, threatening phenomenon. But the results are still disappointing, the reason being the lack of understanding of the "nebulous nature" of cybercriminal acts.*

The article reveals the deep causes and mechanisms of the negative impact of cybercrime on the life of society and on the life of an individual. The close dialectical relationship between cybercrime and information and cyber security is substantiated. The content and conditions of ensuring information and cyber security are revealed. It is argued that intentional or unintentional violation of these conditions constitutes the content of the generic object of cybercrime. In order to solve certain problems in the field of criminal law related to digital technologies, it is proposed to carry out specific studies.

Keywords*: information security, cybersecurity, cybercrime, digital technologies, code.*

Постановка проблеми. В умовах цифрових трансформацій майже вся сукупність суспільних відносин буде реалізовуватись за допомогою цифрових технологій. Така ситуація буде в багатьох сферах суспільного життя: публічного управління, економіки, оборони та безпеки, промисловості, сільського господарства, фінансової та банківської діяльності, енергетики, транспорту, охорони здоров'я, освіти, ретейлу тощо. Широке застосування цифрових технологій вже сьогодні і тим більш в майбутньому є причиною виникнення важливих проблем у сфері боротьби із злочинністю.

Розширення ландшафту кіберзлочинності та одночасно наявність прогалини в розумінні цього явища є серйозною проблемою для правоохоронних органів, особливо

для транскордонних правоохоронних органів, тому за даними UNCTAD (орган ООН, що займається питаннями торгівлі та розвитку) 156 країн (80 відсотків) прийняли законодавство про кіберзлочинність [23].

Особливу увагу слід звернути на результати роботи Міжурядової експертної групи відкритого складу з комплексного дослідження проблеми кіберзлочинності, яку було створено відповідно до Резолюції 65/230 Генеральна Асамблея ООН [45]. В своїй доповіді Міжурядова експертна група дійшла наступних висновків та рекомендацій (2021) [36], зокрема:

1) держави-члени повинні забезпечити, щоб їхні законодавчі положення відповідали вимогам часу з урахуванням технічного прогресу через прийняття законодавства, що містить технічно нейтральні формулювання та передбачає кримінальну відповідальність за діяльність, яку визнають незаконною, а не за використання технічних засобів;

2) державам-членам слід у міру необхідності та доцільності також розглянути питання про розробку на внутрішньодержавному рівні узгодженої термінології для опису кіберзлочинної діяльності та сприяння, наскільки це можливо, точного тлумачення відповідного законодавства правоохоронними та судовими органами;

3) державам-членам слід враховувати той факт, що багато основних положень кримінального законодавства, що застосовуються до офлайнових злочинів, можуть також застосовуватися до злочинів, скоєних в режимі онлайн. У зв'язку з цим державам-членам з метою зміцнення правоохоронної діяльності слід застосовувати, у належних випадках, чинні положення внутрішнього законодавства та міжнародного права щодо злочинів, що скоюються в онлайновому середовищі.

4) державам-членам слід розглянути питання про криміналізацію:

– незаконного отримання доступу до комп'ютерних систем або їх злому;

– незаконного перехоплення або пошкодження комп'ютерних даних та ушкодження комп'ютерних систем;

– незаконного втручання у комп'ютерні дані та системи.

З огляду на рекомендацію щодо урахування технічного прогресу слід зауважити, що цифрові технології збільшують складність кіберзлочинності, яка потенційно здатна завдавати колосальних збитків у майбутньому [39].

Сучасні тенденції поширення цифрових технологій сприятимуть розвитку нових форм кіберзлочинності та зловмисної діяльності. Відбувається: збільшення використання пристроїв IoT, роботів зі здатністю вчитися та навчати інших роботів без втручання людини [39], прогрес у сферах штучного інтелекту, автономних пристроїв і систем, а також телекомунікацій, а також збільшенню обсягу вже існуючих [15], технології віддаленої присутності та віртуальної реальності, квантові обчислювання [34], зростання кількості користувачів соціальних мереж, таких як Facebook, Twitter, LinkedIn, YouTube, WhatsApp, Viber, Messenger тощо [27].

Отже значне розширення сфер використання цифрових технологій, невідворотнє збільшення масштабів цифрової трансформації в сучасних та майбутніх умовах буде мати наслідком зростання кіберзлочинності та кримінальних загроз, тому вивчення проблем кібербезпеки та кримінального права, які можуть мати місце в недалекому майбутньому, не повинно відкладатися або взагалі бути відсутнім [46].

Метою статті є з'ясування технологічної та юридичної природи правопорушень, які відбуваються із застосуванням цифрових технологій, визначення напрямів правових досліджень щодо вдосконалення кримінального законодавства.

Виклад основного матеріалу. В багатьох працях останніх років звертається увага на концептуальні проблеми, які потребують якомога скорішого вирішення. Наведемо деякі з них:

– відсутність ясності щодо поняття "кіберзлочинність", що має значний негативний вплив на суспільство, політику щодо кіберзлочинності, правове втручання та наукові дослідження [18, с. 33];

– жодна з існуючих систем класифікації повністю не враховує концепції кіберзлочинності та точно не відображає туманну природу кіберзлочинних діянь [33];

– прив'язування терміну "кіберзлочинність" до конкретних видів використання технологій або існуючого законодавства про кіберзлочинність перешкоджає повному розумінню поведінки кіберзлочинців та не дозволяє застосувати перспективний підхід, не допускаючи розгляду еволюції або майбутніх явищ кіберзлочинності [33];

– соціальні наслідки передбачуваних нових промислових революцій неминуче стануть загальними визначальними факторами злочинів майбутнього, як це завжди було в минулому [17].

– для сучасної кіберзлочинності характерна транскордонність, що обумовлює проблему наявності юрисдикції різних держав в рамках одного кіберзлочину [17];

– все більш важливою стає гармонізація національних законодавств про кіберзлочинність, яку неможливо досягти без міжнародної співпраці [29, с. 41];

– кіберзлочинність має вивчатись з позиції міждисциплінарних досліджень – кримінального права, соціології, політики, культурології тощо [47].

Не викликає ніяких сумнівів наступний висновок: на основі аналізу законодавства щодо боротьби з кіберзлочинністю виникає більше запитань, ніж відповідей, і беззаперечно, що правова база боротьби з кіберзлочинністю має постійно коригуватися та розвиватися відповідно до надзвичайно швидких і дуже складних технічних викликів [29].

Таким чином, можемо констатувати високу пріоритетність актуальності вирішення проблеми створення теоретико-методологічних засад для встановлення консенсусу у сфері кіберзлочинності. Насамперед, це стосується розуміння "туманної природи" кіберзлочинних діянь та сутності явища кіберзлочинності, взаємозв'язку так званих "кіберзлочинів" та цифрових технологій (комп'ютерних технологій), співвідношення "звичайних" злочинів та злочинів, пов'язаних із цифровими технологіями, місця в загальній класифікації злочинів так званих "кіберзлочинів" тощо. Саме відсутність відповіді на зазначені концептуальні гносеологічні питання у сфері кіберзлочинності стає непереборним бар'єром на шляху вирішення концептуальних проблем забезпечення ефективності боротьби із кіберзлочинами.

Інформаційна безпека.

Якісна (своєчасна, актуальна, повна та достовірна) інформація, ефективність інформаційних відносин та інформаційної взаємодії має фундаментальне значення для прийняття людиною будь-яких рішень. Прийняття оптимальних (раціональних) рішень – це базова умова забезпечення ефективності людської діяльності в будь-якій сфері соціальної активності, що, у свою чергу, є базовою умовою гарантії ефективності функції самозбереження та розвитку цивілізації. Тому питання забезпечення інформаційної безпеки є стратегічно важливим.

В багатьох працях, в національних кримінальних законах кіберзлочини пов'язуються із тематикою інформаційної безпеки. З врахуванням результатів отриманих в працях [9, с. 43] та змісту законодавства України [3] сформулюємо визначення терміну важливого для подальшого аналізу: ***інформаційна безпека*** –

забезпечення такого стану захищеності життєво важливих прав, інтересів і потреб людини, суспільства та держави, при якому мінімізується ймовірність заподіяння шкоди, яка може виникнути як наслідок:

1) *неможливості використання своєчасної, повної, актуальної та достовірної інформації;*

2) *негативного інформаційного впливу;*

3) *порушення штатного режиму функціонування інформаційних технологій;*

4) *несанкціонованого поширення та використання, порушення цілісності, конфіденційності та доступності інформації.*

В запропонованій дефініції окремо визначаються чотири базові умови забезпечення інформаційної безпеки, кожна з яких має свою специфіку. Відомо, що існує безліч вимог щодо ефективного забезпечення визначених базових умов, виконання яких має сприяти забезпеченню інформаційної безпеки. З іншого боку мають місце інформаційні загрози, реалізація яких призводить до нанесення шкоди. ***Загрози інформаційній безпеці*** *– фактори які можуть перешкоджати виконанню базових умов забезпечення інформаційної безпеки та реалізація яких призводить до нанесення шкоди життєво важливим правам, інтересам і потребам людини, суспільства та держави.*

Перша базова умова – наявність можливості використання вчасної, повної, актуальної та достовірної інформації.

Якісна інформація, ефективність інформаційних відносин та інформаційної взаємодії – це базова умова забезпечення ефективності будь-якої особистої, професійної чи суспільної діяльності в будь-якій сфері соціальної активності. А якісна інформація – це своєчасна, повна, актуальна та достовірна інформація, використання якої є необхідним підґрунтям для прийняття рішень, релевантних поставленим цілям діяльності та реальному стану соціальних процесів, внутрішнього і зовнішнього середовища її реалізації, зовнішніх та внутрішніх впливів, а також обставинам, в яких вони приймаються.

В якості прикладу наведемо деякі основні вимоги щодо виконання першої базової умови.

1. *У сфері створення інформації (розвитку інформаційних ресурсів та джерел):*

– визнання на законодавчому рівні одного із базових прав людини – права на своєчасну, повну, актуальну та достовірну інформацію – природнім правом будь-якого суб’єкту інформаційних відносин;

– гарантування свободи слова та вільного вираження своїх поглядів і переконань, зокрема, з використанням цифрових засобів інформаційних комунікацій (соціальних мереж, форумів, чатів тощо);

– створення та підтримання в актуальному стані, зокрема, за допомогою цифрових технологій, загальнонаціональних, галузевих інформаційних ресурсів та баз даних різного тематичного наповнення, наукового та навчального інформаційного ресурсу, реєстрів про населення, нерухомість, землю, інфраструктуру (енергетика, зв’язок, транспортні та газові комунікації тощо);

– формування різноманітних інформаційних джерел за рахунок стимулювання творчої діяльності письменників, молодих вчених, творчих особистостей, студентів тощо;

– забезпечення плюралізму, прозорості, незалежності, конкурентности засобів масової інформації, зокрема, новітніх цифрових медіа;

– сприяння журналістській діяльності, забезпечення гарантії свободи доступу до інформації, нормативного закріплення стандартів журналістської діяльності, зокрема, її незалежності та неупередженості;

– сприяння щодо повсюдного створення та обігу інформації в цифровій формі (електронних документів, книг, журналів тощо);

– врахування правових особливостей використання Інтернет-технологій для поширення масової та будь-якої іншої інформації;

– забезпечення промислового та комерційного обороту неперсоніфікованих та персональних даних;

– захист прав інтелектуальної власності.

2. *У сфері доступу до інформації:*

– забезпечення прозорого та безбар'єрного доступу до будь-якої відкритої інформації та інформації, для якої заборонено встановлювати правовий режим обмеженого доступу;

– встановлення прозорого та безбар'єрного доступу до публічної інформації, зокрема втілення принципу превентивного та проактивного оприлюднення органами публічної влади та місцевого самоврядування всіма можливими засобами комунікацій всього масиву такої інформації;

– забезпечення здійснення превентивних стратегічних комунікацій з народом України кожної інституції всіх рівнів системи органів публічної влади та місцевого самоврядування з метою роз'яснення та обґрунтування важливих питань майбутніх змін у соціально-політичному та економічному житті країни, регіонів, міст та селищ;

– забезпечення доступу до інформації щодо проектів рішень органів публічної влади та місцевого самоврядування задля реалізації конституційного припису щодо реалізації права громадян брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, а також здійснення суспільством незалежного ефективного контролю за їх виконанням;

– гарантування виключення будь-якого обмеження доступу до суспільно значущої інформації:політичної, безпекової, екологічної, стану харчових продуктів, порушення прав людини тощо;

– гармонізації протиріччя між правом на інтелектуальну власність та правом на доступ до інформації тощо.

Без сумніву гарантією виконання першої базової умови забезпечення інформаційної безпеки є надійне функціонування сучасної, розгалуженої інформаційної інфраструктури, яка має забезпечувати ефективне створення, передачу (розповсюдження, поширення), використання та зберігання інформації (інформаційних продуктів) [35].

В якості прикладу наведемо деякі основні вимоги щодо розвитку інформаційної інфраструктури лише тільки в частині передачі інформації:

– формування як конкурентного середовища та подальша лібералізація ринку електронних комунікацій, який характеризується капіталоємністю, високою динамікою зміни технологій та розвиненою топологією мереж, із врахуванням процесів конвергенції, необхідності сумісного ефективного використання ресурсів, зокрема, частотного ресурсу;

– наявність механізмів здійснення державного нагляду за дотриманням вимог законодавства у сфері електронних комунікацій з метою захисту прав та інтересів суб'єктів ринку (споживачів послуг, операторів та держави);

– забезпечення сталого, надійного та якісного функціонування мереж електронних комунікацій та передачі даних;

– розвиток на принципах універсальності доступу та економічної доступності широкосмугових мереж доступу до Інтернету;

– розвиток мереж індустріального Інтернету з особливими вимогами до показників якості передачі даних в інтересах технологій Інтернету речей;

– вдосконалення регулювання діяльності у сфері телебачення та радіомовлення із врахуванням переходу на цифрові технології та на нову парадигму регулювання надання аудіовізуальних послуг;

– створення сприятливих умов діяльності у сфері програмування та виробництва комп'ютерної техніки;

– формування умов інноваційного розвитку технологій Хмарних обчислень та інфраструктури технологій блокчейну тощо.

Друга базова умова – недопущення чи нейтралізація негативного інформаційного впливу.

Існує певна частина інформації, яка внаслідок змісту або форми негативно впливає на людину та її поведінку, що може стати причиною зниження якісних показників діяльності людини, або, іншими словами, може стати причинною виникнення якоїсь шкоди. Небезпечні для людини, її фізичного та психічного стану виклики сучасного світу, які зумовлено різними чинниками, мають якщо не інформаційну природу, то інформаційне підґрунтя чи принаймні виразні інформаційні кореляти[10]. З урахуванням результатів отриманих в праці [11] під ***негативним інформаційним впливом*** *будемо розуміти втручання у свідомість (підсвідомість) або фізичний стан особи чи групи осіб шляхом поширення певної інформації (інформаційних продуктів), що суттєво погіршує їх соціальну поведінку, світогляд та психіку*.

Узагальнюючи висновки [40] можна стверджувати, що негативна інформація складається здебільшого з несприятливих відгуків інших про певні явища, факти чи обставини та безпосередньо впливає на поведінку людей.

Серед негативних інформаційних впливів розрізняють певну кількість однорідних груп. Наприклад, це може бути поширення інформації, яка:

– ганьбить честь і гідність людини (наклеп, дифамація тощо);

– негативно впливає на морально-етичний та психологічний розвиток дитини;

– негативно впливає на морально-психологічний стан окремої людини чи груп людей або завдає шкоди їх фізичному та психічному здоров'ю;

– спотворює уявлення про справжній стан суспільства та навколишнього середовища (дезінформація);

– жорстко детермінує поведінку людини всупереч її реальним інтересам (пропаганда, інформаційна агресія, інформаційна війна) тощо.

В якості прикладу наведемо деякі основні вимоги щодо виконання другої базової умови:

1) законодавче визначення вичерпного переліку видів інформації, відносно якої може бути обмежена свобода доступу та поширення, встановлення чітких, зрозумілих та прозорих правових механізмів такого обмеження для кожного виду інформації, а також визначення судових процедур щодо оперативного розгляду суперечок щодо обмеження.

2) визначення юрисдикції у випадках транскордонного розповсюдження інформації, обмеженої для поширення, а також вдосконалення питань встановлення

юридичної відповідальності суб'єктів інформаційної діяльності за порушення вимог щодо обмеження поширення інформації;

3) встановлення правових засад модерації та промодерації на публічних комунікаційних площадках (телебачення, радіо, соціальні мережі, форуми, месенджери тощо);

4) заборона, нейтралізація та протидія [1]:

– маніпулювання особистісною та суспільною свідомістю, навіювання хибних думок і провокування неправильних дій, завдання шкоди здоров'ю та життю людини тощо;

– розповсюдження недостовірної та шкідливої інформації на шкоду законним інтересам суб'єктів інформаційних відносин, негативного інформаційно-психологічного впливу;

– поширення матеріалів вітчизняних та зарубіжних засобів масової інформації, спрямованих на дискредитацію окремих осіб, підрив суспільної злагоди, дестабілізацію ситуації у країні тощо;

– дезінформації, інформаційному екстремізму та інформаційним війнам.

Третя базова умова – недопущення чи нейтралізація негативних наслідків порушення штатного режиму функціонування інформаційних технологій.

Інформаційні технології *– це сукупність та послідовність методів, способів, засобів та процесів, що використовуються для створення, передачі (поширення, розповсюдження), обробки, використання та зберігання інформації (інформаційних продуктів).* ***Штатний режим функціонування інформаційних технологій –*** *це поточне функціонування інформаційних технологій у відповідності до правових норм та технічних стандартів, вимог технічного завдання та експлуатаційних правил тощо.*

Інформаційні технології, які сьогодні використовується у суспільстві, майже не перелічувані через різноманіття як їх видів, типів, принципів та особливостей технічної реалізації, так і сфер їх застосування. Але переважну більшість сучасних інформаційних технологій об'єднує одне – їх функціонування базується на використанні різноманітних цифрових технологій. Надалі відбуватиметься вдосконалення та модернізація використовуваних цифрових технологій або заміна їх на більш ефективні, але за допомогою яких, як і раніше, будуть реалізовуватись будь-які процеси в людській діяльності.

Складність інформаційних технологій обумовлюється складністю завдань, які виконуються під час різноманітної людської діяльності. Якість та ефективність людської діяльності напряму залежить від правильності (штатного режиму) функціонування інформаційних технологій, які її забезпечують. Тому не викликає сумнівів те, що порушення штатного режиму функціонування цифрових технологій закономірно призводитимуть до зниження ефективності людської діяльності, а іноді й до неможливості її здійснення. Наприклад, порушення штатного режиму функціонування систем автоматизованого керування повітряним рухом цивільних літаків може призвести до повного припинення повітряного сполучення й, навіть, до льотних інцидентів. Порушення штатного режиму функціонування системи керування технологічним процесом атомної станції може призвести до катастрофи. Порушення штатного режиму функціонування комп'ютерної системи керування постачанням мережі маркетів може призвести до нестачі продуктів харчування у місті.

В якості прикладу наведемо деякі основні вимоги щодо виконання третьої базової умови:

1) законодавчо передбачити наявність системи захисту від несанкціонованого втручання та від загроз порушення штатного режиму функціонування інформаційної технології;

2) створення системи захисту має відбуватись одночасно із процесом створення інформаційної технології відповідно до правових норм та технічних стандартів, вимог технічного завдання та експлуатаційних правил;

3) суворе дотримання законодавчо та нормативно встановленого порядку проектування, створення, проведення випробувань, передачі в експлуатацію та експлуатації складних інформаційних технологій, особливо, територіально-розподілених та тих, що забезпечують функціонування об'єктів критичної інфраструктури та техногенно небезпечних об'єктів;

4) застосування правових механізмів щодо забезпечення розробниками (постачальниками) гарантованого супроводження складних інформаційних технологій протягом всього періоду їх експлуатації тощо;

5) встановлення юридичних прав, обов'язків та відповідальності для посадових осіб та персоналу щодо забезпечення штатного режиму функціонування складних інформаційних технологій.

Четверта базова умова – запобігання несанкціонованому поширенню та використанню, порушенню цілісності, конфіденційності та доступності інформації.

В цілому, четверта базова умова зводиться до забезпечення безпеки інформації. ***Безпека інформації*** *– забезпечення такого стану захищеності інформаційної системи, в якій здійснюється її обіг, при якому мінімізується ймовірність заподіяння шкоди, яка може виникнути як наслідок несанкціонованого поширення та використання, порушення цілісності, конфіденційності та доступності інформації.*

Проблематика безпеки інформації відома людству із стародавніх часів, насамперед, як проблема забезпечення таємності та конфіденційності інформації. В подальшому виявилась низка інших проблем, пов'язаних із забезпеченням цілісності та доступності інформації. Виявилось, що реалізація загроз безпеці інформації дедалі частіше та масштабніше призводить до нанесення шкоди життєвим правам, інтересам і потребам людини, суспільства та держави. Шкоди, обсяги якої постійно збільшувались відповідно до збільшення масштабів взаємообумовленої діяльності людей в різних сферах суспільної активності. Тому протягом значного проміжку часу в багатьох державах було напрацьовано досить ефективні системи вирішення переважної більшості проблем забезпечення безпеки інформації. Таки системи, як правило, акцентуються на політичних, державних, суспільних, інституційних, правових, організаційних, технологічних, економічних аспектах забезпечення безпеки інформації.

Саме тим, що проблематика стала добре відомою у суспільстві та досить ефективно функціонують державні системи забезпечення безпеки інформації, пояснюється те, що тривалий час практично всі, навіть, експерти та фахівці, ототожнювали безпеку інформації та інформаційну безпеку. Яскравим прикладом є визначення інформаційної безпеки, що було надано в документі про створення Агентства Європейського Союзу з мережевої та інформаційної безпеки (ENISA) [21]. Цим визначенням інформаційна безпека в Євросоюзі практично була зведена виключно до проблеми забезпечення доступності, достовірності, цілісності та конфіденційності даних, які зберігалися або передавалися за допомогою комп'ютерних мереж та систем. Аналогічне сприйняття інформаційної безпеки як безпеки інформації спостерігається до сьогоднішнього дня у стратегічних документах та законодавстві багатьох держав.

Україна теж має розгалужене законодавство щодо забезпечення безпеки інформації, наприклад такі закони: Конституція України (1996); Про національну безпеку України (2018); Про інформацію (в редакції 2011); Про державну таємницю (1994); Про захист інформації в інформаційно-телекомунікаційних системах (в редакції 2005); Про захист персональних даних (2010); Про доступ до публічної інформації (2011) тощо. Крім того, окремі норми щодо забезпечення безпеки інформації містить низка законів у сфері судочинства, правоохоронної та банківської діяльності, охорони здоров'я, нотаріату, адвокатури, функціонування різноманітних загальнодержавних реєстрів тощо. Для розвитку законодавчих положень прийнята велика кількість підзаконних актів Президентом, Кабінетом Міністрів, окремими центральними органами влади та органами місцевого самоврядування.

Таким чином, існує велика кількість окремих умов, як складових чотирьох базових умов, виконання яких створює системну ситуацію сприяння забезпеченню інформаційної безпеки людини, суспільства та держави. Виконання зазначених умов передбачає реалізацію певної цільової діяльності, визначеними для цього суб'єктами, які приймають участь у відповідних правовідносинах, тобто які мають певні юридичні права, обов'язки та відповідальність.

Будь-які дії, діяльність, події або явища, які перешкоджають виконанню базових та окремих умов, прийнято називати загрозами інформаційній безпеці. Якщо загрози є результатом чи наслідком людської діяльності або бездіяльності, то вони поділяються на навмисні чи ненавмисні.

Дії або бездіяльність щодо недопущення або спотворення виконання базових та окремих умов забезпечення інформаційної безпеки, невиконання або неналежне виконання обов'язків суб'єктами щодо забезпечення інформаційної безпеки можуть мати характер суспільно небезпечних діянь, а значить за певних обставин можуть бути криміналізовані [7].

Кібербезпека.

З врахуванням результатів отриманих автором [37], сформулюємо наступне визначення: ***кібербезпека*** *– це забезпечення такого стану захищеності життєво важливих прав, інтересів і потреб людини, суспільства та держави в умовах використання цифрових технологій, при якому мінімізується ймовірність заподіяння шкоди, яка може виникнути як наслідок:*

1) неможливості використання своєчасної, повної, актуальної та достовірної інформації;

2) негативного інформаційного впливу;

3) порушення штатного режиму функціонування цифрових інформаційних технологій;

4) несанкціонованого поширення та використання, порушення цілісності, конфіденційності та доступності інформації.

Або стисле формулювання: ***кібербезпека*** *– інформаційна безпека в умовах використання цифрових технологій.*

При цьому, ***цифрові технології*** *– це сукупність та послідовність методів, способів, засобів та процесів, що використовуються для створення, передачі (поширення, розповсюдження), обробки, використання та зберігання інформації (інформаційних продуктів) на основі використання комп'ютерів.*

Такий підхід до визначення кібербезпеки створює методологічне підґрунтя для можливого використання всіх напрацювань у сфері у сфері інформаційної безпеки, що є

органічним в умовах використання цифрових технологій. Тому, аналогічно, як і для інформаційної безпеки, для сфери кібербезпеки існує велика кількість окремих умов, як складових чотирьох базових умов, виконання яких створює системну ситуацію сприяння забезпеченню кібербезпеки людини, суспільства та держави. При цьому треба враховувати те, що мета виконання як базових, так і окремих умов є загальною як для інформаційної безпеки, так і для кібербезпеки. Виконання зазначених раніше базових та окремих умов стає актуальним для кібербезпеки лише у випадку використання цифрових технологій в процесі реалізації певної цільової людської діяльності.

Загрози кібербезпеці складають певні навмисні чи ненавмисні дії, які перешкоджають виконанню базових умов забезпечення кібербезпеки, що кореспондуються із виконанням базових та окремих умов інформаційної безпеки.

Але кібербезпека має певні суттєві особливості у порівнянні із інформаційною безпекою. Насамперед мова йде про те, що для першої, другої та четвертої базових умов кібербезпека має розглядатись лише в інфраструктурній конотації, тобто вона не стосується змістовної частини інформації в процесі здійснення інформаційних відносин та інформаційної взаємодії. Виключенням із зазначеного є лише проблема забезпечення цілісності інформації в межах четвертої базової умови кібербезпеки.

Що означає інфраструктурна конотація? З врахуванням результатів отриманих у роботі [35] сформулюємо визначення: ***інформаційна інфраструктура*** *– це сукупність систем та засобів призначених для: виробництва, поширення, обробки, використання та збереження інформації; виконання інформаційних робіт та надання інформаційних послуг; виробництва інформаційних засобів та технологій; сервісного обслуговування інформаційних засобів та технологій; навчання та підготовки персоналу; забезпечення інформаційної безпеки.*

В сучасних умовах значну частину інформаційної інфраструктури складають системи та засоби, які базуються на застосуванні цифрових технологій, тобто комп'ютерів. В такому випадку***, цифрова інформаційна інфраструктура*** *– це інформаційна інфраструктура, функціонування якої базується на застосуванні цифрових технологій, зокрема, мережі Інтернету.* Цифрова інформаційна інфраструктура – це одна із форм реалізації інформаційної інфраструктури, яка в останні роки завдяки використанню цифрових технологій демонструє надзвичайно велике поширення.

В сучасних умовах, створення, передача (поширення, розповсюдження), обробка, використання та зберігання інформації при реалізації будь-якої діяльності в будь-яких сферах соціальної та особистої активності здебільшого відбувається за допомогою цифрової інформаційної інфраструктури, яка служить базою для функціонування як інформаційної, і будь-якої іншої сфери суспільного життя.

До таких цифрових технологій належить також ***Інтернет*** *(мережа Інтернет) як глобальна телекомунікаційна мережа загального користування, призначена для передачі даних між користувачами, яка складається з окремих локальних фрагментів мережі Інтернет та мереж доступу, всі елементи яких логічно пов'язані в рамках глобального адресного простору і взаємодія яких базується на інтернет-протоколі, визначеному міжнародними стандартами.*

Отже, створення, передача (поширення, розповсюдження), обробка, використання та зберігання інформації в сучасних умовах і в майбутньому буде реалізуватись за допомогою Інтернету (мережі Інтернет), як складової цифрової інформаційної інфраструктури.

Треба звернути увагу на те, що застосування та використання цифрових технологій впливає на особливості виконання першої, другої та четвертої базових умов інформаційної безпеки. Зазначені особливості можна згрупувати наступним чином:

– реалізація інформаційних відносин та інформаційної взаємодії за допомогою цифрових технологій, як і будь яких інших технологій, не впливає на зміст інформації, яка передається або зберігається, а також на зміст вхідної інформації, яка обробляється;

– правове регулювання суспільних відносин, які здійснюються за допомогою цифрових технологій, відбуваються відповідно до правового принципу технологічної нейтральності;

– надійність та сталість функціонування сучасної, розгалуженої цифрової інформаційної інфраструктури впливає на ефективність, надійність та сталість будь-якої діяльності;

– використання цифрових технологій при реалізації інформаційних відносин є причиною виникнення проблем правового регулювання, що, наприклад, обумовлено:

– невизначеністю місця розташування сторін інформаційних відносин;

– невизначеністю часу відправлення та отримання інформації сторонами інформаційних відносин;

– певною анонімністю автора інформації, що передається чи розміщується в інформаційних ресурсах, або суб’єкта, який здійснює певні операції з інформацією;

– невизначеністю щодо стану цілісності інформації, що передається, отримується або зберігається.

Нагадаємо, що ***принцип технологічної нейтральності*** *– незалежність змісту правового регулювання суспільних (інформаційних) відносин від технологій, що використовуються для їх реалізації.*

Крім того, інфраструктурна конотація в частині виконання другої базової умови забезпечення інформаційної безпеки означає, що в межах юриспруденції не бажано використовувати поняття на кшталт “кібердезінформація” [28], “кіберпропаганда” [30], “кібернасильство” [48] тому, що цифрові технології у даному випадку використовуються лише для передачі відповідної негативної інформації. Треба зауважити те, що в правовому сенсі для даного випадку першочергове значення має юрисдикція суб’єкта негативного впливу, якій може бути нанесена шкода, а для суб’єкта джерела негативної інформації власна юрисдикція має значення лише у випадку заборони подібних дій.

Отже, всі загрози успішному виконанню базових умов забезпечення кібербезпеки можна об’єднати в наступні групи:

а) недосконаліть цифрової інформаційної інфраструктури в частині її розгалуженості, а також недоліки щодо забезпечення надійності, сталості та захищеності її функціонування;

б) недосконаліть або порушення організаційно-правових та технологічних механізмів недопущення чи нейтралізації реалізації негативного інформаційного впливу;

в) порушення штатного режиму функціонування цифрових інформаційних технологій внаслідок:

– порушення законодавчого та нормативного порядку проектування, створення, проведення випробувань, передачі в експлуатацію та експлуатації складних цифрових інформаційних технологій;

– втручання у функціонування цифрових інформаційних технологій, яке призвело чи могло призвести до порушення його штатного режиму;

г) порушення штатного режиму функціонування спеціальних цифрових інформаційних технологій, призначених для забезпечення захисту від несанкціонованого поширення та використання, порушення цілісності, конфіденційності та доступності інформації в наслідок:

– порушення законодавчо встановленого порядку проектування, створення, проведення випробувань, передачі в експлуатацію та експлуатації спеціальних цифрових інформаційних технологій;

– втручання у функціонування спеціальних цифрових інформаційних технологій, яке призвело чи могло призвести до порушення його штатного режиму.

Зрозуміло, що зазначені групи загроз далі можна поділити на певну множину окремих різноманітних загроз. Важливе зауваження: принципово створення та застосування нових загроз кібербезпеці завжди передує створенню та застосуванню систем захисту від їх дії. Саме тому майже недосяжною є мета стовідсоткового рівня забезпечення кібербезпеки. Це обумовлює стратегію мінімізації шкоди, яка може бути в результаті здійснення загроз, як основне завдання інформаційної безпеки та кібербезпеки.

Кіберзлочинність та кіберзлочини.

На наш погляд, явище кіберзлочинності тісно пов’язано із явищем кібербезпеки. Рівень стану кібербезпеки може бути погіршено в результаті дії навмисних чи ненавмисних загроз, реалізація яких може завдати значної шкоди діяльності людей як на мікро, так і на макрорівні в рамках суверенних держав, а також і в світовому масштабі. Тому кібербезпека передбачає проведення певного комплексу правових, організаційних, організаційно-технічних та техніко-технологічних заходів для її забезпечення з метою унеможливлення або мінімізації реалізації загроз.

Аналіз сутності кібербезпеки свідчить про те, що її проблеми здебільше стосується системних питань функціонування цифрової інформаційної інфраструктури і лише у цих межах вона впливає на особливості виконання першої, другої та четвертої базових умов інформаційної безпеки.

Треба взяти до уваги те, що в результаті здійснення загроз кібербезпеці можуть спостерігатись наступні варіанти нанесення шкоди безпосередньо [37]:

1) технічним системам, які реалізують певну цифрову інформаційну технологію;

2) якісним показникам інформації: своєчасності, актуальності, повноті, достовірності, цілісності, конфіденційності тощо;

3) соціальним або соціотехнічним системам як системам більш високого порядку ієрархії, функціонування яких базується на застосуванні цифрових інформаційних технологій.

Довгий час була поширена практика оцінки розмірів нанесення економічних збитків, яка зосереджувалася на обрахуванні шкоди (збитків) тільки для перших двох варіантів. Лише в останні роки активно здійснюється перехід до третього варіанту, як такого що в переважній більшості випадків релевантно віддзеркалює справжні наміри здійснення загроз. В дійсності ж, треба обраховувати шкоду (збитки) нанесену не лише соціальній або соціотехнічні системі, відносно якої були безпосередньо здійснені загрози, але й нанесену тим соціальним або соціотехнічним систем, що були пов’язані з безпосередньо постраждалою системою у своїй діяльності.

Таким чином, при визначенні рівня суспільної небезпеки певних діянь, пов'язаних із здійсненням загроз кібербезпеці, насамперед, необхідно брати до уваги розмір та масштаби нанесення шкоди соціальним або соціотехнічним системам, зокрема, окремим фізичним особам. І лише саме з цих позицій рекомендується розглядати можливість чи необхідність криміналізації зазначених діянь.

У Конвенції Ради Європи про кіберзлочинність, яку підписали 69 держав]22[, не визначається термін "кіберзлочинність", натомість також визначається певний спектр зловмисних дій, включаючи: незаконний доступ; незаконне перехоплення даних;втручання в дані; втручання в систему; зловживання пристроями; підробка, пов'язана з комп'ютером; шахрайство, пов'язане з комп'ютером;злочини, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторського права та суміжних прав. У додатковому Протоколі [12] до Конвенції про кіберзлочинність зазначається про криміналізацію дій расистського та ксенофобного характеру, вчинених за допомогою комп'ютерних систем.

Доречно звернути увагу на важливу проблему перекладу текстів міжнародно-правових і іноземних актів в українському законодавстві. Англійською назву зазначеного вище Протоколу викладено так: "Additional Protocol to the Conventionon Cybercrime, concerning the criminalisation of act sofa racistan dxenophobic nature committed through computer systems". Наприклад, в Законі України про ратифікацію Протоколу він має назву "Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених ***через*** комп'ютерні системи" [4]. Англійське слово "through" перекладено як "через". Зрозуміло, що вислів "дій …вчинених ***через*** комп'ютерні системи" немає ніякого сенсу з огляду на специфіку функціонування комп'ютерних систем. Подібні переклади спотворюють сенс правової норми і не сприяють розумінню сутності правового регулювання, запропонованого у міжнародно-правових і іноземних актах.

Міжурядова експертна група відкритого складу з комплексного дослідження проблеми кіберзлочинності (2021) [38], з врахуванням чисельних зауважень окремих держав (Австралія, Австрія, ЄС, Китай, Японія, Інтерпол тощо) також рекомендує розглянути питання про криміналізацію окремих суспільно небезпечних діянь.

Такий підхід щодо криміналізації лише окремих суспільно небезпечних діянь не дозволяє сформувати єдину теоретико-методологічну базу для визначення кіберзлочинів, відсутність якої вже сьогодні є бар'єром для формування політики щодо боротьби із кіберзлочинами. В той же час, кіберзлочини являють собою суспільно небезпечне явище, оскільки можуть спричинити втрати компаній на сотні мільярдів доларів [13]. Крім того, кіберзлочинам притаманні висока ймовірність приховування даних, латентність, труднощі в розслідуванні, зумовлені обмеженістю інформації, неможливість уніфікації національних законів і підходів до розслідування у цій сфері, труднощі зі збором даних та їх транскордонним характером тощо[14; 16; 20].

Вважається, що комп'ютерним злочином (кіберзлочином) слід визнавати суспільно-небезпечні діяння, вчинені осудними фізичними особами, які посягають на права, що охороняються законом, та інтереси користувачів інформаційно-телекомунікаційних мереж шляхом порушення систем безпеки функціонування комп'ютерних пристроїв, за допомогою створення, впровадження, використання або поширення забороненої або охоронюваної інформації.

В свій час було надано визначення, яке має універсальний характер: комп'ютерний злочин – це будь-яке злочинне діяння, яке має бути таким, що воно може бути здійснене лише за допомогою комп'ютерної технології [42]. Інше визначення: кіберзлочин у

найширшому розумінні – це будь-яка злочинна діяльність, пов'язана з комп'ютером, мережевим пристроєм або мережею [24].

Таким чином, основна проблема визначення родового об'єкта комп'ютерних злочинів є дискусійною, оскільки аналіз висловлених точок зору дозволяє виділити два взаємовиключних підходи до визначення родового об'єкта комп'ютерних злочинів: безпека використання ЕОМ, систем та комп'ютерних мереж; інформаційні відносини, засобом забезпечення яких є ЕОМ, системи чи комп'ютерні мережі [5]. Але уникаючи складності вирішення зазначених проблем, іноді пропонують всі злочини, під час яких, навіть якщо десь "стояв" комп'ютер, визнавати комп'ютерними.

Однак, з часом стало все більше поширюватись поняття "кіберзлочин". Деякі дослідники вважають поняття "комп'ютерний злочин" і "кіберзлочин" синонімами, а інші переконані, що вони суттєво розрізняються [6]. Здебільшого, при цьому в якості відмінності згадується те, що кіберзлочини відбуваються у кіберпросторі [32].

Яке ж сучасне розуміння кіберпростору? Вважають, що це: нематеріальне середовище, що складається з пристроїв і комунікаційних мереж, яке з'єднує комп'ютери та дозволяє користувачам взаємодіяти один з одним за допомогою комп'ютерно-опосередкованих комунікаційних технологій [44], *віртуальний світ*, створений зв'язками між комп'ютерами, вбудованими пристроями Інтернету, серверами, маршрутизаторами та іншими компонентами інфраструктури Інтернету [25], унікальна сфера штучної людської взаємодії, частково відокремлена від фізичних елементів, яка пронизує традиційні сфери [31].

В Законі України міститься наступне визначення [2]: кіберпростір – середовище (*віртуальний простір*), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Існує інший погляд: кіберпростір – це реалізована комутована мережа для переміщення інформаційного трафіку, яка характеризується різним ступенем доступу, навігації, інформаційної активності, аугментації та довіри, і ці характеристики можна прийняти достатньою мірою для того, щоб зробити правові висновки [26]. Далі автор робить зауваження, яке є суттєвим для сучасного розуміння кіберпростору. Кіберпростір – це не те ж саме, що й Інтернет або телефонна система, які є лише воротами, просто інструментами, які переводять когось у кіберпростір.

Найбільш наближеною до реальності думка К. Чахава: кіберпростір – ***це метафора***, яка використовується для опису глобальної електронної мережі людей, ідей та взаємодії в Інтернеті, яка не обмежена кордонами геополітичного світу [19].

Метафоричність цього терміну, як і багатьох інших, наприклад, таких як віртуальний простір, кіберзлочинність, кіберзлочин, кібердезінформація, кібернасилля тощо, обумовлено надзвичайно швидким масштабним поширенням використання Інтернет-технологій в людському житті. При одночасному надзвичайно низькому рівні знань широких верств населення щодо технічної сутності та особливостей соціального впливу Інтернет-технологій. Саме метафоричність завдяки використанню більш-менш зрозумілої аналогії (кібер та простір) дозволила створити уявну впевненість щодо розуміння "туманної" природи причин та наслідків багатьох нових суспільно важливих явищ, подій, вчинків людей, обумовлених використанням цифрових технологій. Застосування терміну кіберпростір відіграло позитивну роль на певному історичному етапі поширення Інтернет-технологій, але сьогодні використання цього терміну та йому

подібних створює значні перешкоди для релевантного розуміння важливих соціальних явищ та процесів.

Фактично, в наведених прикладах і у роботах багатьох інших дослідників прямо або опосередковано кіберпростір визначається як певний віртуальний простір. Обґрунтування недоцільності та, навіть, шкідливості використання терміну "віртуальний простір" було надано раніше в роботі автора [49], що повністю відноситься й до терміну "кіберпростір".

Таким чином, у процесі рекодифікації кримінального законодавства необхідно врахувати особливості здійснення суспільних відносин, які реалізуються за допомогою цифрових технологій. Особливу увагу потрібно звернути на широке впровадження досягнень четвертої промислової революції у різних сферах: технологій Інтернету речей, Індустрії 4.0, штучного інтелекту, робототехніки, Великих даних, Хмарних обчислень, електронних комунікацій, а також технологій генної інженерії, нано- та біотехнології тощо.

Крім того, потрібно враховувати сутність та суспільне значення інформаційної безпеки і кібербезпеки, вимоги та системні заходи щодо їх забезпечення тощо, навмисне чи ненавмисне порушення умов забезпечення яких складає зміст родового об'єкту кіберзлочину. Зазначене потребує проведення ретельних та ґрунтовних теоретико-методологічних та практичних правових досліджень із залученням результатів міждисциплінарних досліджень в зазначених вище сферах.

Для вирішення проблем в галузі кримінального права, які пов'язані із цифровими технологіями, доцільно провести наступні дослідження:

1) щодо визначення окремих систем соціальних цінностей, яким спричиняється шкода коли:

– знаряддям вчинення кримінального правопорушення є виключно лише цифрові технології;

– знаряддям вчинення кримінального правопорушення можуть бути цифрові технології поряд з іншими, що визначаються проектом Кримінального кодексу (далі – Кодекс)[8];

– цифрові технології є виключно допоміжним засобом для знарядь вчинення кримінального правопорушення, які визначено таким Кодексом;

2) щодо можливості вдосконалення визначення "потерпілої особи" (Кодекс), враховуючи те, що до соціальних цінностей, яким завдається шкода, можна віднести права та інтереси окремих груп людей, суспільства та держави, а також інтереси системи міжнародного правопорядку;

3) щодо можливості визнання в якості спеціального предмету кримінального правопорушення – соціального або технологічного процесу (виборчий процес, процес голосування, процес державного управління, процес функціонування атомних станцій, системи керування повітряним рухом, цифрових технологій тощо;

4) щодо вдосконалення терміну "способу вчинення кримінального правопорушення", визначеного Кодексом, додавши до нього: "а також система дій, метод чи прийом, що визначаються законодавством із забезпечення інформаційної безпеки та кібербезпеки";

5) щодо можливості вдосконалення визначення "знаряддя вчинення кримінального правопорушення" (Кодекс) додавши до нього цифрові технології;

6) щодо можливості вдосконалення визначення "місце вчинення кримінального правопорушення" (Кодекс) додавши до нього речення: "Місцем вчинення кримінального правопорушення із застосуванням в якості знаряддя цифрових

технологій особою, яка знаходиться під юрисдикцією держави Україна, але перебуває за межами держави та не має житла чи іншого приміщення в Україні";

7) щодо необхідності внесення до приватного та публічного законодавства норм, діяння з порушення яких можна буде вважати протиправним.

Звичайно, цей перелік проблем є далеко не вичерпним. Усвідомлення надзвичайної важливості застосування цифрових технологій у всі сфери життя окремої людини, суспільства та держави потребує пильної уваги та відповідної реакції представників науки кримінального права.

Висновки.

В умовах масштабної цифрової трансформації проблема кіберзлочинності набуває надзвичайної ваги та актуальності. Вирішення цієї проблеми в сучасних умовах інформаційної глобалізації та транскордонної взаємодії може стати можливим лише на засадах принципово нового підходу до оновлення кримінального законодавства не тільки в межах національних правових систем, а насамперед на рівні міжнародного права.

Новий підхід має спиратись на консенсусне розуміння технічної та технологічної природи правопорушень, які відбуваються із застосуванням цифрових технологій. Саме єдина позиція щодо розуміння технологічних особливостей скоєння злочинів, пов'язаних із цифровими технологіями, дозволить сформувати узагальнене бачення особливостей суспільних відносин, які відбуваються за цих обставин. З огляду на універсальність цифрових технологій, які не мають національного забарвлення, їх застосування у такому випадку також не буде вносити національного забарвлення до особливостей реалізації суспільних відносин. Це відкриває шлях до можливої міжнародної універсалізації правового регулювання у сфері кримінальних злочинів, які відбуваються із застосуванням цифрових технологій.

Зміна парадигми розгляду злочинів, пов'язаних із цифровими технологіями, створить підґрунтя для швидкого формування відповідного зрозумілого та прозорого міжнародного кримінального права, на основі якого в майбутньому бажано провести гармонізацію національних кримінальних законодавств.

Використана література

1. Довгань О., Ткачук Т. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація та право*. № 1(29)/2019. С. 86-99.

2. Про основні засади забезпечення кібербезпеки України: Закон України. Верховна рада України. 5 жовтня 2017 р.

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України. Верховна Рада України. 2007.

4. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Закон України. Верховна Рада України. 21 липня 2006 р.

5. Карчевский Н. Компьютерныепреступления: определение, объект и предмет: матеріали V Международной конференции *Право и Интернет: теория и практика,* 25-26 нояб. 2003 р.

6. Номоконов В., Тропина Т. Киберпреступность: угрозы, прогнозы, проблемы борьбы. *Information Technology and Security*. 2013. № 1. С. 86-94.

7. Панов М., Харітонов С. Суспільна небезпечність діяння – фундаментальна ознака поняття "кримінальне правопорушення". *Юридична Україна*. 2019. № 10. С. 13-20.

8. Проект нового Кримінального кодексу України EUAM. 2022. URL: https://new criminalcode.org.ua/criminal-code (дата звернення: 13.11.2022).

9. Баранов О. Інформаційне право України: стан, проблеми, перспективи. СофтПрес, 2005. 316 с.

10. Слюсаревський М. Негативні інформаційні впливи на людину в сучасному світі: концептуальна модель: матеріали семінару *Актуальні проблеми психологічної протидії негативним інформаційним впливам на особистість в умовах сучасних викликів,* м. Київ, 8 квіт. 2021 р.

11. Сніцаренко П. Аналіз стану виявлення та оцінювання негативного інформаційного впливу на особовий склад Збройних Сил України в системі протидії такому впливу: збірник наукових праць Центру воєнно-стратегічних досліджень. 2019. № 2. С. 52-61.

12. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Council of Europe. 28 January 2003.

13. Alghamdie M. A novel study of preventing the cybersecurity threats. Materials Today: Proceedings. 2021. n. pag.

14. Babanina V., et al. Cybercrime: History of formation, current state and ways of counteraction. Amazonia Investiga. 2021. 10(38). P. 113-122.

15. Bellasio J., etc. The future of cybercrime in light of technology developments. 2020. URL: https://www.rand.org/pubs/research_reports/RRA137-1.html (дата звернення: 13.11.2022).

16. Баранов О. Проблеми законодавчого забезпечення боротьби з комп‘ютерними злочинами: зб. наук. праць *Інформаційні технології та захист інформації*. Запоріжжя: Юридичний інститут МВС України. 1998. Вип. 2. С. 3-13

17. Bjelajac Ž., Filipović A. Specific characteristics of digital violence and digitalcrime. *Pravo - Teorija I Praksa.* 2021. № 38(4). P.16-32.

18. Calcara G., Peter S., Matti T. Cybercrime, law and technology in Finland and beyond. 2019. 154 p. URL: https://www.theseus.fi/handle/10024/166377 (дата звернення: 13.11.2022).

19. Chakhava K. Terrorist Psychology and Its Impact on International Security. World Politics and the Challenges for International Security. IGI Global. 2022. P. 165-185.

20. Баранов О.А. Кримінологічні проблеми комп’ютерної злочинності: зб. наук. праць *Інформаційні технології та захист інформації*. Запоріжжя: Юридичний інститут МВС України, 1998. Вип. 2. С. 64-69.

21. Concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. European Parliament and of the Council. May 21, 2013.

22. Conventionon Cybercrime. Council of Europe. Budapest. November 23, 2001.

23. Cybercrime Legislation Worldwide UNCTAD. 2020. URL: https://unctad.org/page/cyber crime-legislation-worldwide (дата звернення: 13.11.2022).

24. Dinarević M., Lejla S. Razvoj, pojamioblici cyberkriminala / Development, Concept and Forms of Cyber Crime. Pregled: časopiszadruštvenapitanja. 2021.: n. pag.

25. Dingalo L. The Increased Need for Cybersecurity in Developing Countries: COVID-19 and the Adverse Cybercrime Risks Imposed. Cybersecurity Capabilities in Developing Nations and Its Impacton GlobalSecurity. IGI Global. 2022. P. 218-236.

26. Folsom, T. Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). Tul. J. Tech. &Intell. Prop. 2007. 9. P. 75121.

27. Giri S., Subarna S. High Risk of Cybercrime, Threat, Attack and Future Challenges in Nepal. International Journal of Computer Sciences and Engineering. 2020. 8.2. P. 46-51.

28. Hunt J. Counter in gcyber-enabled disinformation: implications for national security. *Australian Journal of Defence and Strategic Studies*. 2021. № 3-1. P. 83-88.

29. Khan S., et al. A systematic literature review on cybercrime legislation. F1000 Research 2022. 11.971. P. 971.

30. Maseri A., et al. Socio-Technical Mitigation Effortto Combat Cyber Propaganda: A Systematic Literature Mapping. IEEE Access. 2020. № 8. P. 92929-44.

31. Medeiros B., Goldoni L. The Fundamental Conceptual Trinityof Cyberspace. *Contexto Internacional*. 2020. № 42. P. 31-54.

32. Mphatheni M., Maluleke W. Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International journal of research in business and social science*. 2020. № 11(4). P. 384-96.

33. Phillips K., et al. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*. 2022. 2.2. P. 379-98.

34. Project 2020 Scenarios for the Futureof Cybercrime. ICSPA. 2013. URL: chrome-exten sion://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europol.europa.eu/sites/default/files/documents /2020_white_paper.pdf (дата звернення: 13.11.2022).

35. Баранов А. Информационная инфраструктура: проблемы регулирования деятельности. Видавничий дім Дмитра Бураго, 2012. 352 с.

36. Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime. UNODC. 2021. HeldinVienna from 6 to 8 April. URL: chrome-extension://efaidnbm nnnibpcajpcglclefindmkaj; https://www.unodc.org/documents/organized-crime/cybercrime/ Cybercrime-April-2021/Report/V2102595.pdf (дата звернення: 13.11.2022).

37. Баранов О. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*. № 2(42)/2014. С. 54-62.

38. Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime. UNODC. HeldinVienna from 6 to 8 April 2021.

39. Seneviratne D. Emerging Technologies: The Future of Cybercrime. 2017. URL: https://www. researchgate.net/publication/341600490_Emerging_Technologies_The_Future_of_Cyber crime (дата звернення: 13.11.2022).

40. Shih M., Shu-Hui C. How in fluential is negative informational influence? Evidence from online consumer changes in attitudes. *Bioinformatics*, 2016. № 15(12). P. 7290-96.

41. Siregar G., Sarman S. The Law Globalization in Cybercrime Prevention. *International Journal of Law Reconstruction* . 2021. 5.2. P. 211-27.

42. Tavani H. Defining the boundariesof computer crime: piracy, break-ins, and sabotagein cyberspace. SIGCAS Comput. Soc. 2000. 30. P. 3-9.

43. Баранов А. Информационный суверенитет или информационная безопасность. *Національна безпека і оборона*, 2001. № 1. С. 70-76.

44. Tonellotto M. Crime and victimization in cyberspace: a socio-criminological approach to cybercrime. In Handbook of Researchon Trendsand Issuesin Crime Prevention, Rehabilitation, and Victim Support. IGI Global. 2020. P. 248-64.

45. Twelfth United Nations Congresson Crime Prevention and Criminal Justice resolution 65/230. UN. General Assembly. 2010. 21 December. URL: chrome-extension://efaidnbmnnnibpca jpcglclefindmkaj; https://www.unodc.org/documents/Cybercrime/General_Assembly_resolution_65-230_ E.pdf (дата звернення: 13.11.2022).

46. Wang X. Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics*: Conference Series. 2020.1533 3.

47. Yar M., Steinmetz K. Cybercrime and Society. 2013. URL: https://books.google.pl/books/ about/Cybercrime_and_Society.html?id=_nN7DwAAQBAJ&redir_esc=y (дата звернення: 13.11.2022).

48. Zarnoufi R., Mehdi B., Mounia A. AI top reventcyber-violence: harmful behaviour detection in social media. Int. J. High Perform. Syst. Archit. 2020. 9.4. P. 182-191.

49. Баранов О. Віртуальність і правове регулювання. *Публічне право*. 2017. № 1. С. 210-218.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~