МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Олеся БОДУНОВА

ТЕОРЕТИКО-ПРИКЛАДНІ ОСНОВИ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Монографія

Луцьк
Вежа-Друк
2023

УДК 343.85:004.056](477)
Б 75

Рекомендовано до друку вченою радою
Державного податкового університету
(протокол № 14 від 29 червня 2023 року)

Рецензенти:
Леган І. М., доктор юридичних наук, доцент, професор кафедри права та правоохоронної діяльності Державного університету «Житомирська політехніка»;
Корнякова Т. В., доктор юридичних наук, професор, заслужений юрист України, завідувач кафедри адміністративного і кримінального права Дніпровського національного університету ім. Олеся Гончара;
Дідківська Г. В., доктор юридичних наук, професор, завідувач кафедри кримінальної юстиції Державного податкового університету.

Бодунова Олеся
Б 75 Теоретико-прикладні основи запобігання злочинності у сфері інформаційних технологій : монографія / Олеся Бодунова. – Луцьк : Вежа-Друк, 2023. – 344 с.

ISBN 978-966-940-526-5

У монографії висвітлено поняття інформаційної безпеки як одного з основних напрямів кримінологічної політики України, визначено стан наукових досліджень злочинності у сфері інформаційних технологій, охарактеризовано генезис дослідження проблематики злочинності у сфері інформаційних технологій, представлено наукове уявлення про сучасний стан злочинності у сфері інформаційних технологій, визначено поняття злочинності у сфері інформаційних технологій**,** сформовано кримінологічний портрет особи злочинця, що вчиняє кримінальні правопорушення у сфері інформаційних технологій, охарактеризовано види кримінальних правопорушень у сфері інформаційних технологій, висвітлено нормативно-правове забезпечення запобігання цього виду злочинності, а також запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні.

Монографія буде корисною для наукових, науково-педагогічних, практичних працівників та здобувачів вищої освіти.

УДК 343.85:004.056](477)

© Бодунова О. М., 2023
© Олейник А. В. (обкладинка), 2023

ISBN 978-966-940-526-5

ЗМІСТ

ПЕРЕДМОВА 5
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ГНОСЕОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ .9
1.1. Інформаційна безпека як один з основних напрямів кримінологічної політики України 9
1.2. Стан наукових досліджень злочинності у сфері інформаційних технологій 29
1.3. Генезис дослідження проблематики злочинності у сфері інформаційних технологій 46
1.4. Методологія дослідження злочинності у сфері інформаційних технологій 63
Висновки до Розділу 1 77
РОЗДІЛ 2. КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ 79
2.1. Кількісні та якісні показники злочинності у сфері інформаційних технологій 79
2.2. Поняття злочинності у сфері інформаційних технологій .. 95
2.3. Кримінологічний портрет особи злочинця, що вчиняє кримінальні правопорушення у сфері інформаційних технологій 113
2.4. Класифікація кримінальних правопорушень у сфері інформаційних технологій 135
Висновки до Розділу 2 153
РОЗДІЛ 3. ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ 155
3.1. Сучасний стан запобігання злочинності у сфері інформаційних технологій 155
3.2. Нормативно-правове забезпечення запобігання злочинності у сфері інформаційних технологій 179
3.3. Суб’єкти запобігання злочинності у сфері інформаційних технологій в Україні 199
3.4. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні 213
Висновки до Розділу 3 232

РОЗДІЛ 4. ЗАРУБІЖНИЙ ДОСВІД ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ В УКРАЇНІ 235

4.1. Досвід окремих зарубіжних країн щодо запобігання злочинності у сфері використання інформаційних технологій 235

4.2. Міжнародно-правові стандарти запобігання злочинності у сфері інформаційних технологій 251

4.3. Формування моделі забезпечення інформаційної безпеки в мережі internet на основі позитивного досвіду зарубіжних країн 273

Висновки до Розділу 4 292

ВИСНОВКИ 294

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 302

ПЕРЕДМОВА

Сьогодні глобальна всесвітня мережа, що об'єднує мільйони комп'ютерів у транснаціональну єдину систему Інтернет, відкриває широкі можливості для спілкування та обміну інформацією будь-якого характеру. Це зумовило виникнення нового типу суспільних відносин – відносин у кіберпросторі, що підносять на якісно новий рівень розвитку всі сфери життєдіяльності, зокрема економіку, державне управління, мистецтво, науку, освіту тощо. Втім, нарівні з позитивними здобутками Інтернет-середовище характеризується побічними, негативними явищами криміногенного характеру, до яких відносять порушення авторських прав, розповсюдження та збут творів, що пропагують культ насильства і жорстокості, порнографічних предметів, наркотичних засобів, вимагання, шахрайство через Інтернет та інші види як традиційних, так і власне кримінальних правопорушень у сфері інформаційних технологій. Технологія вчинення таких кримінально протиправних діянь із використанням ІТ-технологій та мережі Інтернет надзвичайно ускладнює процес розслідування порівняно з виявленням такої категорії кримінальних правопорушень, що вчиняються у звичайних умовах.

Особливу небезпеку такі кримінальні правопорушення становлять в умовах воєнного стану, адже окрім активних бойових дій триває й повномасштабна інформаційна війна російської федерації проти України. Так, кіберзлочинці активно використовують інформаційний простір для взлому урядових серверів, розповсюдження дезінформації серед населення та створення фейкових профілів у соціальних мережах тощо. Кібершахрайство, під час якого злочинці, видаючись представниками різних служб і організацій, намагаються отримати банківські реквізити громадян для незаконного заволодіння їх коштами, стало дуже розповсюдженим.

Таким чином, війна в інформаційному просторі завдає суспільству не менших збитків, ніж збройний конфлікт на полі бою. З урахуванням цього, в Україні вже розпочато процес вдосконалення чинного кримінального та кримінального процесуального законодавства щодо запобігання цьому виду злочинності. Проте на сьогодні цей процес не є ефективним, оскільки кіберзлочинці постійно вдосконалюються у виборі методів вчинення кримінальних правопорушень.

Окрім цього, одним із проблемних питань запобігання злочинності у сфері інформаційних технологій є те, що такі кримінально протиправні діяння часто перетинають кордони і можуть бути вчинені з будь-якої точки світу. Це ускладнює процес виявлення і притягнення винних осіб до відповідальності. Тому важливо приділяти належну увагу кібербезпеці, розробці та впровадженню правових норм, що регулюють кіберзлочини, та надавати поліції та правоохоронним органам належні повноваження для їх запобігання.

Все це підкреслює важливість обраної теми і необхідність дослідження чинного законодавства, правозастосовної практики і наукових джерел з цього питання.

Актуальність обраної теми також підтверджується офіційними статистичними даними. Так, кількість кримінальних правопорушень у сфері інформаційних технологій з кожним роком постійно зростає. Зокрема, з огляду на статистичні дані Офісу Генерального прокурора, станом на 31 грудня 2022 року обліковано 3 415 кримінальних правопорушень у сфері інформаційних технологій, що на 105 кримінальних правопорушень більше порівняно з 2021 роком та на 917 – більше порівняно з 2020 роком. Це свідчить в цілому про суттєве зростання, а саме – на 3,1 % порівняно з 2021 роком та – на 26,8 % порівняно з 2020 роком, кількості зареєстрованих кримінальних правопорушень[1].

Не зменшується кількість випадків кібершахрайства у фінансовому секторі, зокрема, пов'язаного з виплатами «фейкової» благодійної допомоги. Так, упродовж дії воєнного стану слідчими Національної поліції України розпочато 789 кримінальних проваджень за фактами незаконних дій, пов'язаних з гуманітарною допомогою, благодійними пожертвами та безоплатною допомогою з наступною правовою кваліфікацією: стаття 201-2 КК України 630; стаття 190 КК України – 60; стаття 191 КК України – 34; за іншими статтями КК України – 65[2].

Проблемам впливу інформаційно-комунікаційних технологій на суспільне життя, інформаційній безпеці, кіберзлочинності та кібербезпеці присвячені роботи багатьох учених. Різні аспекти

[1] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

[2] Офіційний сайт Національної поліції України: URL: https://www.npu.gov.ua/diyalnist/zvitnist

згадуваної проблематики розглядаються у роботах таких вітчизняних та зарубіжних учених, як Д. С. Азаров, Ю. М. Батурин, І. Р. Березовська, О. І. Бугера, В. В. Гостєв, М. В. Гуцалюк, М. А. Дем'янчук, В. М. Дрьомін, Д. В. Дубов, В. М. Желіховський, В. А. Залізняк, С. В. Кавун, О. В. Климчук, А. А. Комаров, А. П. Леонов, В. А. Ліпкан, Ю. Є. Максименко, В. В. Марков, В. А. Мисливий, Ю. М. Онищенко, В. В. Остроухов, В. М. Петрик, К. С. Пивоварська, М. М. Присяжнюк, Н. А. Розенфельд, І. С. Стаценко-Сургучова, Т. В. Скубіна, Т. Л. Тропіна, А. В. Тунік, Д. М. Цехан, В. Т. Шатун та інших.

Безпосередньо запобігання злочинності у сфері інформаційних технологій досліджувалося такими науковцями як: В. С. Бабійчук, В. М. Бутузов, С. А. Буяджи, Б. М. Головкін, Г. В. Дідківська, М. В. Карчевський, О. Г. Колб, А. М. Коломієць, М. О. Кравцова, Н. А. Лугіна, Ю. В. Нікітін, Н. Б. Новицька, В. А. Номоконов, Д. Паркер, В. В. Пивоваров, Є. Я. Прохоренко, О. О. Проскурін, Н. З. Рогатинська, Н. В. Сметаніна, О. В. Таволжанський, Ш. Шольберг, С. Хантінгтон, О. Е. Радутний, В. В. Топчій, Т. Л. Тропіна, Г. М. Чернишов, С. В. Шапочка, В. М. Шевчук, В. Ю. Шепітько, Н. С. Юзікова, О. М. Яхно.

Вищевказані науковці, безперечно, зробили вагомий внесок у теорію і практику розвитку правової доктрини щодо запобігання злочинності у сфері інформаційних технологій, їхні праці заклали теоретичні засади розроблення нових обґрунтованих пропозицій щодо покращення ефективності застосування таких механізмів та наукових концепцій з цього питання. Водночас аналіз їхніх напрацювань свідчить про те, що проведені дослідження стосувалися в основному лише окремих доктринальних і прикладних питань запобігання злочинності у сфері інформаційних технологій в Україні. На сьогодні залишаються недостатньо дослідженими і такими, що не знайшли достатнього правового урегулювання, питання щодо поняття, сутності та ознак злочинності у сфері інформаційних технологій, запобігання цьому виду злочинності в умовах воєнного стану, формування оновленої моделі запобігання злочинності у сфері інформаційних технологій на основі вивчення позитивного досвіду зарубіжних країн тощо.

У монографії висвітлено поняття інформаційної безпеки як одного з основних напрямів кримінологічної політики України,

визначено стан наукових досліджень злочинності у сфері інформаційних технологій, охарактеризовано генезис дослідження проблематики злочинності у сфері інформаційних технологій, представлено наукове уявлення про сучасний стан злочинності у сфері інформаційних технологій, визначено поняття злочинності у сфері інформаційних технологій**,** сформовано кримінологічний портрет особи злочинця, що вчиняє кримінальні правопорушення у сфері інформаційних технологій, охарактеризовано види кримінальних правопорушень у сфері інформаційних технологій, висвітлено нормативно-правове забезпечення запобігання цього виду злочинності, а також запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні.

Монографія буде корисною для наукових, науково-педагогічних, пракичних працівників та здобувачів вищої освіти.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ГНОСЕОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1. Інформаційна безпека як один з основних напрямів кримінологічної політики України

Активна інформатизація українського суспільства є важливим напрямком сучасної діяльності, яка має як позитивні, так і негативні аспекти. Позитивні аспекти інформатизації включають в себе полегшення доступу до інформації, адже інтернет надає можливість швидко і зручно отримувати доступ до різноманітної інформації, навчатися і отримувати новини з усього світу; покращення комунікації, оскільки інтернет дозволяє людям спілкуватися миттєво навіть на великих відстанях, що полегшує роботу, освіту та особисті стосунки; розвиток економіки, бо інформатизація сприяє створенню нових інноваційних галузей, розвитку електронної комерції і підвищенню продуктивності праці в багатьох галузях.

Однак, разом з позитивними аспектами інформатизації інформаційне суспільство також стикається з негативними викликами, а саме зі злочинністю у сфері інформаційних технологій. Сьогодні зростає кількість кіберзлочинів, таких як кібершахрайство у фінансовому секторі, крадіжка даних, атаки на комп'ютерні системи тощо; порушується приватність та безпека, оскільки збільшення збору та обробки особистої інформації може порушувати приватність та піддавати загрозі безпеку даних; інтернет стає платформою для поширення фейкових новин і дезінформації, що може впливати на суспільну думку і рішення.

Інформатизація в Україні також супроводжується зростанням комп'ютерної злочинності. Боротьба з цими проблемами вимагає вдосконалення законодавства, забезпечення кібербезпеки та розвитку кадрового потенціалу для боротьби з кіберзлочинами. Так, починаючи з 2018 року працівники Національної поліції України були залучені до більше ніж одинадцяти тисяч кримінальних проваджень, пов'язаних з вчиненням кримінальних правопорушень у сфері новітніх інформаційних технологій. Найбільша кількість протиправних діянь вчиняється в Києві, на території Одеської, Миколаївської та Львівської областей [219]. І на сьогодні, в умовах воєнного стану,

інформаційні технології є одним із основних способів реалізації кримінально протиправної мотивації.

Варто зазначити, що такі негативні тенденції поширились ще з початку окупації російською федерацією АРК Крим, Донецької та Луганської областей. На той час було відомо, що тільки за декілька місяців 2016 року на об'єктах п'яти відомств і 31 державного інформаційного ресурсу було здійснено близько 6500 спланованих кібератак. За звітом американської компанії Microsoft, після початку широкомасштабного збройного вторгнення російської федерації в Україну 24.02.2022 року, російські хакери вчинили майже 240 кібератак проти України – підприємств та державних установ. Атаки часто були спрямовані на знищення комп'ютерних систем, але деякі також були спрямовані на збирання розвідувальних даних або поширення дезінформації [219 с. 249–252].

Звіти про таку велику кількість кібератак на Україну свідчать про серйозну загрозу кібербезпеці в регіоні. Кібератаки можуть мати різний характер і мету, включаючи руйнівні атаки, збирання розвідувальної інформації, дезінформацію і інші види кіберагресії.

Поряд з цим, професор Г. Г. Почепцов вказує на важливість когнітивної безпеки, особливо в умовах сучасного інформаційного суспільства. Когнітивна безпека охоплює заходи, спрямовані на захист розумових процесів та розвиток навичок критичного мислення в суспільстві. Пропаганда та маніпуляція інформацією можуть серйозно впливати на сприйняття реальності та призводити до негативних наслідків [227]. Зміна сприйняття та ментальних операцій може мати серйозні наслідки для індивіда та суспільства в цілому.

Пропаганда і маніпуляція інформацією використовуються для впливу на когнітивні процеси людей шляхом створення специфічних інформаційних повідомлень, які можуть активувати певні схеми і упередження в мозку. Це може призводити до зміни сприйняття реальності та вироблення небажаних переконань і поглядів. Для того, щоб захистити себе від такого впливу, важливо розвивати критичне мислення, стежити за різними джерелами інформації та аналізувати інформацію незалежно. Також важливо розвивати навички медіаграмотності, щоб розрізняти добросовісні джерела від маніпулятивних і сприймати інформацію з обережністю.

Держави також можуть грати важливу роль у захисті когнітивної безпеки громадян, встановлюючи правила та стандарти для

інформаційних платформ, сприяючи незалежному журналістському розслідуванню та розповсюдженню правдивої інформації. Боротьба з маніпулятивною інформацією вимагає спільних зусиль громадян, активістів і урядових органів. [227]. Тобто, когнітивна операція, безперечно, спрямована на зміну моделі світу людини [226, с. 170].

Доцільно відмітити, що у когнітивній війні людська свідомість стає полем бою. Мета полягає в зміненні не лише того, що думає людина, а й того, як вона думає і діє. Саме тому науковці наполягають на важливості концепції когнітивної війни і когнітивної безпеки (COGSEC), яка демонструє актуальність усвідомлення того, як інформація може бути використана для впливу на думки, переконання та поведінку людей в сучасному інформаційному середовищі. Когнітивна війна – це форма конфлікту, в якій психологічний інформаційний вплив використовується для досягнення стратегічних методів. Когнітивна безпека (COGSEC) передбачає заходи для захисту індивідуальних та колективних когнітивних процесів від негативного впливу, включаючи маніпуляцію інформацією, дезінформацію, пропаганду та інші форми психологічного впливу. Основною метою COGSEC є збереження інтегритету когнітивної системи і забезпечення об’єктивності та незалежності при прийнятті рішень [267].

Ці заклики пролунали в контексті оголошення російською федерацією інформаційної війни європейським країнам та США. Термін «когнітивна безпека» вживається, аби підкреслити загрози й ризики, які пов’язані з пізнавальною діяльністю, негативними впливами ЗМІ, перебуванням людини у віртуальній реальності [281].

Професор М. В. Маркова зазначає, що інформаційно-психологічний вплив може викликати зрушення в цінностях, життєвих позиціях, орієнтирах, світогляді особистості [199, с. 7]. Такі зміни зумовлюють вияви девіантної антисоціальної поведінки й становлять небезпеку вже для суспільства й держави. Медіа-аналітик К. Ілюк також наголошує, що інформаційно-психологічний вплив завжди здійснюється з метою зміни поведінки. Тобто, кожен фейк, провокація чи спекуляція у своїй сукупності має штовхати до дії [142].

У публікації 2014 р. латвійський дослідник Янис Берзиньш (Jānis Bērziņš) наголошував, що «російський погляд на сучасну війну ґрунтується на ідеї, що основним полем бою є погляди, і, як наслідок, у війнах нового покоління має домінувати інформаційно-

психологічна війна з метою змусити військове та цивільне населення супротивника підтримати нападника на шкоду власному уряду та країні» [378, с. 5–13].

Повномасштабне вторгнення російської федерації в Україну та її активні дії у сфері інформаційної війни дійсно висувають інформаційну безпеку на перший план у питаннях національної та міжнародної безпеки. російська федерація використовує інформаційну війну як частину своєї гібридної стратегії для досягнення своїх цілей в Україні та впливу на інші демократичні країни.

Спроби маніпулювати інформацією, дезінформувати та використовувати соціальні мережі для поширення пропаганди становлять серйозну загрозу національній та міжнародній стабільності. Інформаційна війна може призводити до підриву довіри до демократичних інституцій, втрати громадянської згуртованості та загрози національній безпеці. Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» було встановлено, що «інформаційна політика російської федерації – загроза не лише для України, але й для інших демократичних держав. Спеціальні інформаційні операції російської федерації спрямовуються на ключові демократичні інституції (зокрема, виборчі), а спеціальні служби держави-агресора намагаються посилити внутрішні протиріччя в Україні та інших демократичних державах. Застосовані російською федерацією технології гібридної війни проти України, у тому числі, моделі і механізми інформаційного втручання поширюються на інші держави, швидко адаптуючись до локальних контекстів та регуляторних політик. Обмежувальні заходи (санкції) та ефективний механізм моніторингу і відповідальності за їх порушення є одним із дієвих механізмів відповіді на дезінформаційну активність російської федерації як держави-агресора [256].

Як ми уже зазначали, спеціальні інформаційні операції, що проводяться російською федерацією проти України, становлять серйозну загрозу національній безпеці та суверенітету України. Ці операції включають в себе розповсюдження дезінформації, фейкових новин та маніпуляції громадською думкою з метою підірвати довіру до українських владних структур, створити панічні настрої в суспільстві, спровокувати прояви екстремізму та загострити соціально-політичну ситуацію в Україні.

Також російська федерація використовує інформаційні кампанії для легітимізації анексії Криму та дестабілізації українського суспільства. Ці кампанії можуть включати в себе поширення спростувань щодо своєї участі в конфлікті на сході України, а також спроби вплинути на міжнародну спільноту з метою зняття санкцій проти Росії.

Для боротьби з цими загрозами Україна має розвивати систему стратегічних комунікацій, підвищувати інформаційну грамотність громадян та сприяти незалежному журналізму. Також важливо продовжувати співпрацю з міжнародними партнерами для обміну інформацією та координації заходів для запобігання дезінформації й інформаційній агресії.

Для захисту своєї інформаційної інфраструктури та забезпечення свободи слова на тимчасово окупованих територіях Україна повинна прикладати зусилля щодо підтримки журналістів та медіа організацій, які працюють в цих умовах.

Варто зазначити, що в Україні вже є певні напрацювання з цього приводу. Створення ефективної системи координації та взаємодії між органами державної влади України у сфері стратегічних комунікацій є критично важливим для забезпечення ефективного захисту національного інформаційного простору та національної безпеки. Для досягнення цього можна розглянути декілька можливих кроків:

1) *створення центрального координаційного органу*: уряд України може створити центральний орган або комітет, відповідальний за координацію інформаційних зусиль у сфері стратегічних комунікацій. Цей орган може об’єднувати представників різних міністерств та інших органів для забезпечення єдиної стратегії та координації дій.

2) *розробка стратегії інформаційної безпеки*: Україна повинна розробити оновлену національну стратегію інформаційної безпеки, яка визначатиме загальні цілі та пріоритети в цій сфері. Ця стратегія має враховувати внутрішні та зовнішні загрози та визначати конкретні заходи для їх протидії.

3) *створення механізмів обміну інформацією*: важливо встановити механізми обміну інформацією між різними органами та агентствами, які займаються інформаційною безпекою. Це надасть змогу вчасно реагувати на загрози та координувати заходи.

4) *підвищення інформаційної грамотності*: уряд може запровадити програми для підвищення інформаційної грамотності серед населення, що допоможе громадянам відрізняти правдиву інформацію від дезінформації та фейкових новин.

5) *захист інформаційної інфраструктури*: для забезпечення захисту національної інформаційної інфраструктури важливо розглянути введення сучасних технологій та кіберзахисту.

6) *співпраця з міжнародними партнерами*: Україна може співпрацювати з міжнародними організаціями та партнерами для обміну досвідом та інформацією щодо інформаційної безпеки.

Варто зазначити, що багато країн мають правові норми та регулюють питання інформаційної безпеки та захисту особистих даних через різні закони та нормативи:

1) Директива Європейського Союзу про захист даних (EUDPD): ця директива має на меті захист особистих даних громадян ЄС та встановлює стандарти для захисту конфіденційності даних на всій території ЄС. Країни-члени ЄС повинні розробити національні правила, які відповідають цій директиві.

2) Закон про права сім'ї на освіту і недоторканність приватного життя 1974 р. (FERPA) у США: цей закон захищає конфіденційність записів про освіту учнів. Закон визначає права здобувачів вищої освіти та вимоги до конфіденційності освітніх записів.

3) Закон про підзвітність медичного страхування (HIPAA) 1996 р. у США: HIPAA регулює конфіденційність та безпеку електронних медичних записів і транзакцій у сфері охорони здоров'я та медичного страхування.

4) Закон Гремма-Ліча-Блаєла (GLBA) 1999 р. у США: цей закон регулює конфіденційність і безпеку приватних фінансових даних, отриманих фінансовими установами.

5) Стандарт безпеки даних індустрії платіжних карт (PCI DSS): PCI DSS встановлює стандарти безпеки для захисту платіжних даних та протидії шахраївству з використанням платіжних карт.

6) Закон про захист особистої інформації та електронної документації в Канаді: цей закон захищає особисті дані під час їх передачі та зберігання в електронній формі.

7) Закон про захист даних 1998 р. у Великобританії: цей закон регулює обробку даних про фізичних осіб та їх конфіденційність.

8) Закони про інформаційну безпеку в Греції: грецькі закони встановлюють мінімальні стандарти контролю інформаційної

безпеки в сфері електронного зв'язку та захисту інфраструктури [298, с.110–115].

Розглянувши світовий досвід правового регулювання відносин з приводу інформаційної та кібернетичної безпеки, варто вказати й на українські нормативно-правові джерела у цій галузі.

Потрібно почати з того, що протягом 2020–2021 рр. в Україні прийнята низка безпекових стратегій, зокрема: Стратегія національної безпеки України від 14.09.2020 р., затверджена Указом Президента України від 14.09.2020 р. No 392/2020; Стратегія воєнної безпеки України від 25.03.2021 р. (Указ від 25.03.2021 р. No 121/2021); Стратегія кібербезпеки України від 14.05.2021 р. (Указ від 26.08.2021 р. No 447/2021); Стратегія інформаційної безпеки від 15.10.2021 р. (Указ від 28.12.2021 р. No 685/2021).

Окрім цього, на сьогодні це питання регулюється низкою законів:

– Закон України «Про основні засади забезпечення кібербезпеки України» визначає особливості і напрямки забезпечення захисту прав та інтересів у кіберпросторі;

– Закони України «Про національну безпеку України» і «Про концепцію національної програми інформатизації» містять положення про специфіку забезпечення національної інформаційної безпеки;

– Закони України «Про інформацію» та «Про захист економічної конкуренції» дають визначення поняттю інформації;

– Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». У цьому нормативно-правовому акті висвітлені актуальні питання щодо взаємодії уповноважених державних органів стосовно забезпечення інформаційної безпеки, системи їх повноважень щодо захисту інтересів українців і країни в цілому в інформаційній сфері.

М. Т. Гаврильців розрізняє норми в інформаційній сфері залежно від їх призначення та змісту, зокрема:

1) норми, що закріплюють завдання і напрямки діяльності країни в інформаційному середовищі: ця категорія включає в себе нормативні акти, які визначають основні завдання і напрямки діяльності держави в інформаційній сфері. Сюди входять статті Конституції України та інші закони, які встановлюють загальні принципи розвитку інформаційного простору країни;

2) норми про порядок взаємодії органів влади із суб'єктами інформаційних відносин: ця категорія включає норми, які визначають порядок співпраці між державними органами і суб'єктами інформаційних відносин, включаючи процедури державного регулювання в даній сфері. Наприклад, закони про телебачення, радіомовлення, доступ до публічної інформації тощо;

3) норми щодо адміністративно-правового статусу суб'єктів інформаційних відносин: ця категорія включає норми, які визначають правовий статус суб'єктів, які беруть участь у інформаційних відносинах. Наприклад, закони про телекомунікації можуть встановлювати права та обов'язки операторів зв'язку;

4) норми щодо системи органів державного регулювання в інформаційному середовищі: ця категорія включає норми, які стосуються системи органів державного регулювання в інформаційному просторі, а також їхнього адміністративно-правового статусу. Сюди можуть входити положення Конституції та інші законодавчі акти, що регулюють органи влади в інформаційній сфері [90, с. 202].

Окрім урегулювання основних засад інформаційної безпеки в Україні, метою прийняття цих нормативно-правових актів є удосконалення та визначення понятійного апарату.

Погоджуємося з А. Іленковим у тому, що термінологія займає особливе місце в збереженні та передаванні знань, оскільки саме на неї припадає основне інформаційне навантаження [14, с. 24–29].

Як зазначає автор, з поняттям «інформаційна безпека» «склалася парадоксальна ситуація. З одного боку, термін «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та нормативних документах різного рівня, з іншого боку, це поняття досі не має однозначного розуміння» [13, с. 7].

Як зазначає D. Schatz, є досить мало розумінь поняття «кібербезпека», що потенційно може викликати значні проблеми в контексті організаційної стратегії, бізнес-цілей або міжнародних угод [392, с. 54].

Почнемо з того, що термін «інформаційна безпека» закріплений у законодавстві України.

Так, згідно ч. 1 ст. 17 Конституції України, захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу[168].

Також сутність інформаційної безпеки України за змістом у контексті інформаційної діяльності було визначено у Концепції (основах державної політики) національної безпеки України, схваленій [245].

Згідно з цим нормативним актом, забезпечення інформаційної безпеки в Україні передбачає:

1) реалізацію комплексних заходів для захисту власного інформаційного простору та включення України в глобальний інформаційний простір;

2) виявлення та ліквідацію причин інформаційної дискримінації, що стосується України;

3) припинення негативних впливів, спрямованих на порушення інформаційного простору та інформаційну експансію з боку інших держав;

4) розробку та впровадження необхідних засобів і режимів для отримання, зберігання, поширення та використання суспільно значущої інформації;

5) створення розвинутої інфраструктури в сфері інформаційних технологій;

6) інформаційна безпека є невід'ємною складовою національної безпеки і включає в себе різні аспекти, такі як політична, економічна, оборонна і інші.

З метою уточнення і упорядкування поняття інформаційної безпеки законодавство надає орієнтовний перелік об'єктів, які є частиною цієї безпеки. Цими об'єктами є інформаційні ресурси, канали обміну інформацією та телекомунікації, механізми, які забезпечують функціонування телекомунікаційних систем і мереж, а також інші складові інфраструктури інформаційної системи країни.

Поняття інформаційної безпеки в контексті інформатизації отримало правове визначення в Концепції Національної програми інформатизації, затвердженій Законом України від 4 лютого 1998 року № 75/98-ВР. Згідно з цим законом, інформаційна безпека охоплює комплекс нормативних документів, які стосуються використання обчислювальної техніки для обробки і зберігання обмежено доступної інформації, включаючи стандарти документування, супроводження, використання та сертифікацію програмних засобів для захисту інформації, засоби для діагностики, локалізації і

профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи і багато іншого [170].

Згідно з Розділом IV Концепції національної програми інформатизації, створення умов для інтеграції України у світовий інформаційний простір має відбуватися з урахуванням сучасних тенденцій інформаційної геополітики з метою забезпечення обороноздатності та державної безпеки.

У науковій літературі поняття «інформаційна безпека» може мати різне тлумачення, аналогічне до поняття «безпека». Представимо декілька наукових інтерпретацій цього поняття.

Інформаційна безпека розглядається як забезпечення захисту інформації від несанкціонованого доступу, розповсюдження і використання. Це включає заходи з шифрування, автентифікації, контролю доступу тощо. Інформаційна безпека може бути спрямована на запобігання кібератакам і іншим загрозам для інформаційних систем і мереж, що може вплинути на діяльність організацій або країни в цілому. Інформаційна безпека може також включати в себе аспекти забезпечення конфіденційності, цілісності і доступності інформації, а також захист від дезінформації і маніпуляційної інформації. Ці інтерпретації ілюструють різноманітні підходи до розуміння інформаційної безпеки в науковій сфері.

Думка В. Я. Рубана підкреслює важливість інформаційної безпеки як стану, в якому людина, суспільство і держава мають високий рівень інформаційної готовності. Ця готовність включає духовний, інтелектуальний, морально-етичний і політичний аспекти.

За такого стану інформаційної безпеки жодні негативні інформаційні впливи не здатні спричинити деструктивні думки і дії, які можуть вести до негативних відхилень на шляху стійкого і прогресивного розвитку цих суб'єктів (особи, суспільства, держави).

Це підкреслює важливість створення позитивного інформаційного середовища, де індивіди мають здатність критично оцінювати інформацію, розуміти її вплив на свої погляди і вчинки, і відстоювати свої цінності та інтереси в умовах інформаційного впливу. Такий підхід сприяє стійкому розвитку та зміцненню індивідів, суспільства і держави в контексті інформаційної безпеки [279, с. 170].

Погляди В. Голубєва та О. Ющука на інформаційну безпеку, як стан інформаційної озброєності, дійсно розширюють поняття безпеки на психологічний, інтелектуальний, морально-етичний та політичний рівні. Це підкреслює важливість не лише захисту фізичної безпеки від зовнішніх загроз, але й збереження стійкості індивідів, суспільства і держави перед інформаційними впливами, які можуть призвести до негативних наслідків. Науковці розуміють під цим поняттям такий стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи неспроможні на них викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів [97, с. 25].

Категорія «інформаційна безпека» в організаційному та управлінському аспекті може бути розглянута як стан захищеності життєво важливих інтересів особи, суспільства і держави. Забезпечення інформаційної безпеки включає в себе заходи та політику, спрямовану на запобігання ризикам та загрозам, пов'язаним із збитками, що можуть виникнути через певні загрози [279, с. 174].

Автори книги «Організація і сучасні методи захисту інформації» пропонують таке визначення категорії «інформаційна безпека» – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування і розвиток в інтересах громадян, організацій і держави. Варто зазначити, що саме це визначення у більшій мірі використовується як категорія науки державного управління [216, с. 52].

Також в літературних джерелах вживається така категорія, як «безпека інформаційної системи» – заходи, які охороняють інформаційну систему від несанкціонованого доступу, випадкового чи зловмисного втручання в нормальні дії або намагання зруйнувати її компоненти.

Звернемо увагу на те, що більшість науковців дає визначення «інформаційна безпека», обгрунтовуючи свої висновки на основі базового освітнього досвіду та використовуючи певні критерії.

Л. Ірвін під інформаційною безпекою розуміє заходи, що призначені для захисту цінних активів, таких як бізнес-записи, особисті дані, результати інтелектуальної творчості та інші види

інформації. Ці дані можуть бути збережені на різних носіях інформації, таких як сервери, жорсткі диски, хмарові сховища, особисті пристрої, паперові документи і так далі [376].

Інформаційна безпека, на думку технічного фахівця Дж. Фрулінгера, – це набір методів, призначених для захисту даних від несанкціонованого доступу або змін, як при зберіганні, так і при передачі з одного приладу або фізичного розташування на інше. Іноді під інформаційною безпекою також розуміють безпеку даних (від англ. Data security) [373].

Обговорювана захищена інформація може приймати будь-яку форму, в тому числі, електронну або фізичну; матеріальну (документація) або нематеріальну (знання). Саме збалансований захист конфіденційності, цілісність і доступність даних – це об'єкти захисту інформаційної безпеки. При цьому основний акцент зроблено на ефективній реалізації політики певної організації, без зниження продуктивності такого суб'єкта.

Варто зазначити, що найчастіше для забезпечення інформаційної безпеки використовується структурований процес управління ризиками, який включає в себе:

1) оцінку ризиків: цей етап включає в себе ідентифікацію потенційних загроз та визначення вразливостей в інформаційній системі. Це допомагає встановити, які інформаційні активи підлягають захисту та які загрози можуть їм загрожувати;

2) прийняття рішення: на цьому етапі вирішується, які методи боротьби з ризиками будуть прийняті. Це може включати в себе прийняття заходів забезпечення безпеки, перерозподіл ризиків або прийняття ризику на основі стратегічних вагомостей;

3) виявлення загроз і вразливостей: цей етап передбачає активний моніторинг та аналіз нових загроз та вразливостей, які можуть виникати у зв'язку з розвитком технологій або змінами в діловому середовищі;

4) відстеження активності: цей аспект включає в себе постійний моніторинг безпеки та відстеження подій та інцидентів, щоб вчасно реагувати на можливі загрози;

5) розробка і впровадження заходів безпеки: останній етап полягає в розробці та впровадженні конкретних заходів безпеки для зниження ризиків. Вони можуть включати в себе технічні заходи, політики безпеки, навчання персоналу та інші заходи.

Загалом, інформаційна безпека – це набір методів і стратегій, які спрямовані на захист конфіденційної інформації від різних загроз і ризиків, і вона є критично важливою для сучасних організацій і організаційних структур.

Поряд із тим, в науковій літературі опублікована велика кількість робіт, які, використовуючи поняття «інформаційна безпека», фактично спрямовані на певні локальні питання з цієї сфери, наприклад: «інформаційна безпека» підприємств і безпеки господарської діяльності [1, с. 11;], «інформаційна безпека» бібліотеки [29], «інформаційна безпека» в органах внутрішніх справ [107, с. 739], «інформаційна безпека» страхових компаній [126, с. 33] та ін. Варто зазначити, що ці визначення не в повній мірі відображають сутність інформаційної безпеки, а лише частково її характеризують з огляду на ту чи іншу сферу діяльності.

Також відмітимо, що в деяких випадках дослідження «інформаційної безпеки» зводиться до аналізу проблематики «кібербезпеки» [77, с. 210].

У науковій статті Н. М. Волошиної розглядається співвідношення понять «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. Зазначається, що «на перший погляд, «безпека інформації» та «інформаційна безпека» тотожні за змістом, але насправді це далеко не відповідає істині [87, с. 55]. У праці «інформаційна безпека» розглядається на підставі міждисциплінарного підходу: як в контексті «захисту інформації», так і в контексті «захисту від інформації» [341, с. 301].

Важливий аспект інформаційної безпеки відображає думка В. М. Фурашева, який полягає в тому, що для споживача результати неповної, невірогідної, упередженої або спотвореної інформації можуть бути схожими, незалежно від причин цих недоліків. Основними наслідками такої інформації є невірогідність сприйняття, спотворення уявлень та негативний вплив на прийняття рішень [328, с. 57].

Варто зазначити, що загрозами інформації у кіберпросторі є кіберзагрози, а відтак засобами протидії цим загрозам є заходи забезпечення кібербезпеки [298]. У цьому сенсі слід зазначити, що в Стратегії від 15.10.2021 р. не заперечується роль кібербезпеки як виду або форми інформаційної безпеки.

Порівнюючи розуміння «інформаційної безпеки» у Стратегії та в програмному документі ЮНЕСКО «Інформація для всіх» (IFAP) з

2001 року, можна відзначити, що вони мають спільні аспекти і підходи до захисту інформації, але також мають свої особливості.

У програмному документі ЮНЕСКО IFAP визначено різні аспекти інформаційної безпеки, такі як захист конфіденційної інформації, збереження світової інформаційної спадщини, захист від інформації негативного характеру, безпека даних особистого характеру, сумлінне використання інформації, та захист прав інтелектуальної власності. Ці аспекти стосуються загальних принципів та цілей інформаційної безпеки, які мають захищати інформацію від різних загроз та використовувати її відповідально та етично [29, с. 18].

У Стратегії від 15.10.2021 року більше наголошено на небезпеці деструктивного впливу і спеціальних інформаційних операцій. Це відображає більш сучасний підхід до інформаційної безпеки, де важливість захисту від суттєвого впливу на інформацію та інформаційні процеси стає зрозумілою у зв'язку з розвитком цифрових технологій, масовим поширенням інтернету і соціальних медіа, та активністю кіберзлочинців і державних акторів.

Важливою є не лише захист інформації, але і збереження її цілісності, доступності та недоступності для несанкціонованих осіб чи сутностей. Сучасні загрози можуть бути більш складними та різноманітними, і відповідно до цього і стратегії та підходи до інформаційної безпеки стають більш комплексними.

Отже, хоча обидва документи мають спільні аспекти, Стратегія від 15.10.2021 року враховує сучасні виклики та реалії інформаційної безпеки, включаючи деструктивний вплив і спеціальні інформаційні операції, та наголошує на їх важливості.

Саме тому поняття «інформаційна безпека» не може зводитися до безпеки окремої сукупності даних чи інформаційних систем чи до кібербезпеки, хоча ці поняття і пов'язані між собою. Так, Є. О. Архипова у згаданій вище статті вказує, що «інформаційна безпека» є ширшим за обсягом поняттям, ніж «безпека інформації» і включає в себе останню. Ототожнення цих понять вона пов'язує із тим, що вітчизняні дослідники не враховують, що міжнародні стандарти, з яких запозичується визначення терміну information security, належать до сфери безпеки інформаційних технологій, де об'єктом захисту виступає саме інформація (а не людина, суспільство чи держава). Таке формальне запозичення призводить до суттєвої плутанини в термінологічних визначеннях [13, с. 9].

Так, дослідниця зазначає, що у стандарті BS ISO/IEC 17799 Information security характеризується забезпеченням конфіденційності, цілісності та доступності інформації, а в ISO/IEC 27001 – як «всі аспекти, пов'язані з визначенням, досягненням та підтримкою конфіденційності, цілісності, доступності, невідмовності, підзвітності, автентичності та достовірності інформації чи засобів її обробки». Дж. Фрулінгер (J. Fruhlinger) також звертає увагу на так звану тріаду ЦРУ як основні складові безпеки інформації: конфіденційність, цілісність і доступність. Усі ці міркування стосуються виключно поняття «безпека інформації» [373].

Згідно ч. 1 ст. 1 Закону України «Про інформацію», інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [244]. Отже, захисту підлягає інформація не тільки в електронному вигляді, а на будь-якому носії. Зокрема, Abi Tyas Tunggal та Kaushik Sen наголошують, що «незалежно від того, як зберігається ваша інформація, вашій організації потрібні відповідні засоби контролю безпеки, щоб запобігти несанкціонованому доступу» [354].

Поряд з терміном «інформаційна безпека», досить часто використовується поняття «кібербезпека». Багато науковців визначають їх як терміни-синоніми, хоча ці визначення різняться між собою.

Згідно з Д. Шацом, Дж. Волл і Р. Башроушу, кібербезпека (вона ж комп'ютерна безпека і безпека інформаційних технологій) – це захист комп'ютерних систем і комп'ютерних мереж від розкриття даних, пошкодження та крадіжки їх обладнання, програмного забезпечення або електронної інформації, а також від порушення або неправильного спрямування наданих ними послуг [392].

Також можна говорити і про те, що кібербезпека – це використання сучасних технологій, процесів і засобів контролю з метою захистити комп'ютерні системи та мережі, програми, пристрої і дані від кібернетичних атак, а також з метою зниження ризику здійснення кібератаки [401].

Система кібербезпеки складається із декількох елементів, координація яких всередині організації має вирішальне значення для успіху всієї програми кібербезпеки. Ці елементи включають такі елементи: безпеку додатків; безпеку даних; безпеку критично важливої інфраструктури; мережеву і операційну безпеку; хмарну

безпеку; планування аварійного відновлення, а разом із ним і забезпечення безперервності бізнесу; фізичну охорону; навчання кінцевих користувачів.

Підтримка кібербезпеки стає все більш важливим завданням для організацій, оскільки поява нових кіберзагроз вимагає більш активного та адаптивного підходу. Традиційні методи захисту інформації та мережевих систем можуть виявитися недостатніми для ефективного запобігання сучасним загрозам. Для забезпечення інформаційної безпеки потрібно більше, ніж просто захист основних елементів системи; необхідно брати до уваги всі аспекти і компоненти, включаючи допоміжні.

У зазначених категоріях інформаційної безпеки (технічна та організаційна) мета залишається однаковою: захист інформації та запобігання загрозам в комп'ютерних і мережевих системах. Однак, їхні підходи відрізняються:

Технічна інформаційна безпека в основному зосереджена на технологічних заходах та рішеннях для захисту систем, мереж та даних. Це може включати у себе встановлення файрволів, антивірусного програмного забезпечення, шифрування даних та інші технічні заходи.

Організаційна інформаційна безпека ставить більший акцент на аспектах управління та людському фактору в безпеці. Це включає в себе створення культури інформаційної безпеки в організації, навчання співробітників правилам інформаційної безпеки, визначення політик та процедур безпеки, а також управління ризиками [390, с. 179].

У зв'язку із вищезазначеним варто вказати на результати дослідження, проведеного Verizon Wireless, найбільшим оператором стільникового зв'язку США. Згідно з його звітом із розслідування витоків даних за 2020 рік, 30 % інцидентів порушення кібербезпеки пов'язані із внутрішніми суб'єктами всередині компанії. Дослідження включало в себе вивчення 3950 порушень [352]. Таким чином, забезпечення культури інформаційної безпеки є першочерговим завданням кожної держави.

Отже, обидва ці терміни важливі, але вони спрямовані на захист різних аспектів безпеки в інформаційному середовищі.

Кібербезпека зосереджена на захисті цифрових активів, таких як дані, системи, мережі, сервери, програми та інші цифрові ресурси. Вона націлена на запобігання кібератакам, втручанню та несанкціонованому доступу до цих активів. Кібербезпека включає в себе

технічні, організаційні та процедурні заходи для забезпечення безпеки в цифровому середовищі [371].

Інформаційна безпека, з іншого боку, охоплює ширший спектр аспектів, включаючи не лише цифрові активи, але і фізичні та людські аспекти. Вона націлена на захист інформації у будь-якій формі, будь то електронні, паперові або усна інформація. Інформаційна безпека включає в себе заходи щодо забезпечення конфіденційності, цілісності та доступності інформації, а також заходи для запобігання іншим загрозам, таким як соціальний інженерінг, фізичний доступ та інші.

Таким чином, кібербезпека є підмножиною інформаційної безпеки, і вони співіснують, забезпечуючи комплексний захист інформації та цифрових ресурсів в сучасному інформаційному середовищі.

Отже, під інформаційною безпекою ми розуміємо стан захищеності систем обробки і зберігання інформаційних даних, при якому гарантовано конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційних впливів.

Натомість кібербезпека – це вужче поняття і означає діяльність, спрямовану на захист інформації, комп’ютерних систем і мереж від кібератак та охоплює весь комплекс заходів щодо керування паролями до інструментів комп’ютерної безпеки на основі технологій машинного навчання.

Фахівці з кібербезпеки зазвичай спеціалізуються на захисті цифрових активів та мережі. Вони виявляють потенційні вразливості у системах та мережах, розробляють та впроваджують заходи безпеки, виявляють і виправляють інциденти кібербезпеки та запобігають кібератакам. Фахівці з кібербезпеки забезпечують, щоб технічні аспекти безпеки були належним чином налаштовані і відслідковувалися. Повноваження фахівців з інформаційної безпеки, з іншого боку, можуть включати в себе більш широкий спектр обов’язків. Вони можуть визначати загальну політику інформаційної безпеки для організації, розробляти плани відновлення після кібератак, вести навчання персоналу щодо питань інформаційної безпеки, визначати

процедури і політику збереження даних, а також співпрацювати з іншими відділами, щоб забезпечити загальну інформаційну безпеку в організації [374].

Варто зазначити, що справді існують подібності між інформаційною безпекою і кібербезпекою, і це може призводити до плутанини в застосуванні цих термінів. Деякі подібності між ними включають:

1) методи і заходи: обидва типи безпеки використовують схожі методи і заходи для захисту інформації. Це включає в себе розробку політик безпеки, шифрування даних, виявлення і виправлення вразливостей, моніторинг мережі тощо;

2) фізична безпека: інформаційна безпека і кібербезпека можуть включати компонент, який стосується фізичної безпеки інформації. Це означає захист фізичних медіа, таких як сервери, диски, паперові документи і так далі, для запобігання фізичному доступу до інформації;

3) оцінка цінності інформації: обидва підходи зазвичай оцінюють цінність інформації для організації. Це допомагає визначити, яку інформацію слід захищати в першу чергу і які ресурси слід спрямовувати на її захист [377].

Ми погоджуємося з позицією І. М. Сопілко у тому, що доцільно розглядати кібербезпеку в якості форми, підмножини інформаційної безпеки, як її складового елементу на рівні з криптографією і подібними категоріями [298].

Інформаційна безпека і кібербезпека хоча і мають різні акценти, проте є критично важливими аспектами для організацій і держави в цілому. Вони спільно спрямовані на захист даних, і обидва поняття важливі для захисту від різних загроз, як цифрових, так і фізичних.

Культура інформаційної безпеки є не менш важливою, і вона передбачає усвідомлення персоналом масштабів загроз та відповідальність за безпеку в їхній роботі. Постійне поліпшення методів та вдосконалення підходів до інформаційної безпеки і кібербезпеки є ключем до ефективного захисту.

Важливо, що влада приділяє належну увагу розробці та впровадженню нових методів і стандартів безпеки, а також співпрацює з міжнародними партнерами для обміну досвідом і гармонізації законодавства. Це допомагає забезпечити ефективний захист інформації та кіберпростору в умовах зростаючих загроз і викликів у цій сфері [27, с. 80].

Отже, проаналізувавши визначення інформаційної безпеки, кібербезпеки можна зробити такі висновки.

Законодавче закпілення дефініції інформаційної безпеки України добре відображає сутність цього поняття та його комплексний характер. Інформаційна безпека справді включає в себе захист прав і свобод людини у сфері інформації, а також запобігання поширенню недостовірної, об'єктивної інформації, боротьбу з негативними інформаційними впливами, деструктивною пропагандою і іншими загрозами інформаційній безпеці.

Ця концепція також включає в себе заходи для захисту цілісності інформації, щоб запобігти її перекрученню та несанкціонованому поширенню. Інформаційна безпека стає дедалі важливішою, особливо в цифрову епоху, коли обмін інформацією став надзвичайно швидким і широким.

Проте в умовах воєнного стану виникли нові загрози інформаційній безпеці України. Так, ситуації у сфері інформаційної діяльності в Україні відображають низку серйозних проблем і викликів, з якими стикаються журналісти та ЗМІ в країні. Дійсно, актуальними є такі проблеми:

1) обмеження свободи медіа: обмеженням свободи ЗМІ і професійної діяльності журналістів може стати загрозою свободі слова і доступу громадян до інформації. Це може призвести до недостатнього висвітлення суспільно важливих подій і обмеження прав громадян на отримання об'єктивної інформації.

2) посягання на безпеку журналістів: погрози, насильство та інші форми посягання на безпеку журналістів є серйозною проблемою, яка може вплинути на їхню здатність виконувати свою професійну діяльність і інформувати суспільство.

3) залежність ЗМІ від власників: залежність засобів масової інформації від їх власників може призвести до впливу власників на редакційну політику і обмеження незалежності ЗМІ.

4) додержання журналістських стандартів: важливо забезпечити дотримання журналістських стандартів, що включають етичні та професійні норми. Це допоможе зберегти довіру громадськості до ЗМІ та журналістів.

У нашій державі склалася неоднозначна ситуація, коли російські ЗМІ проштовхують абсолютно недемократичні принципи розвитку нашої держави, формуючи, таким чином відповідну думку лояльних до держави-агресора громадян України, що завдає значної шкоди

інтересам нашої держави у її демократичного розвитку. З огляду на зазначені обставини, можна зауважити, що вище згаданий указ є необхідним для захисту національних інтересів України і спрямований саме на зупинення розповсюдження російської пропаганди у нашій державі. Тому усі закиди щодо обмеження свободи діяльності ЗМІ на території України є недоцільними та такими, що не відповідають дійсності. До того ж, цілком можна погодитись із твердженням, що в умовах війни російська федерація активно розпочала упереджене та викривлене висвітлення фактів та явищ не лише для свого населення, але й безпосередньо для всього світу, що в результаті призвело до антиукраїнського руху. Такі дії сприяли пропаганді ідей сепаратизму, насильства, національної ворожнечі суспільства, яскравим прикладом якого є самопроголошені утворення так званих ДНР та ЛНР на території унітарної України. Слід зазначити, що засоби масової інформації вже давно на практиці визнаються четвертою гілкою влади, яка має безперечно вагомий вплив на засоби масової комунікації та може здійснювати маніпуляції з суспільною думкою. Сьогодні преса робить те, що століття тому робили священики та церква. Телебачення, газети, радіо, інформаційні агенції грають першу скрипку у ментальній ідеологічній сфері [313, с.155].

У військових конфліктах і воєнному стані інформаційна сфера може бути використана для маніпулювання суспільною думкою, дестабілізації суспільства та впливу на внутрішню і зовнішню політику держави. Інформаційні загрози можуть включати дезінформацію, пропаганду, кібератаки, обмеження доступу до інформації, а також інші способи впливу на інформаційні ресурси та інфраструктуру. Забезпечення інформаційної безпеки передбачає створення системи захисту від таких загроз, розвиток кіберзахисту, контролю за розповсюдженням дезінформації, забезпечення надійності інформаційної інфраструктури та ресурсів держави, а також вдосконалення системи контрінформації та інформаційної боротьби [68].

Отже, державна політика щодо забезпечення інформаційної безпеки є важливою складовою національної безпеки. В її основі повинна бути системна превентивна діяльність органів державного управління щодо надання гарантій інформаційної безпеки особистості, соціальним групам, суспільству і державі в цілому.

Аналіз свідчить про існування реальних загроз інформаційній безпеці України [112, с. 158].

Отже, проблема інформаційної безпеки як кримінологічної категорії пов'язана з численними аспектами та вимагає взаємозв'язку з іншими проблемами, включаючи національну безпеку та захист інтересів як громадян, так і держави. В умовах тривалого конфлікту і воєнного стану важливо розглядати інформаційну безпеку як один із ключових елементів загальної системи захисту та захисту національних інтересів.

Інформаційна безпека може відігравати критичну роль у запобіганні нанесенню шкоди шляхом упередженого інформування, маніпуляційної інформації та інших форм впливу на свідомість та поведінку громадян. Вона також може сприяти укріпленню стійкості суспільства до інформаційних атак та допомагати у виявленні та боротьбі з дезінформацією та іншими інформаційними загрозами.

Запобігання неправдивому та незаконному висвітленню інформації, її контроль та регулювання, а також розвиток інформаційної грамотності серед громадян є важливими компонентами інформаційної безпеки. У цій сфері співпраця між державою, громадськістю, ЗМІ та іншими стейкхолдерами може грати ключову роль у вирішенні цих завдань.

1.2. Стан наукових досліджень злочинності у сфері інформаційних технологій

Терміни, пов'язані з префіксом «кібер-», є предметом наукової дискусії і поки що не мають чіткого та універсального визначення на міжнародному та національному рівнях. Поняття кіберзлочинності, кіберзлочинів, злочинності у сфері інформаційних технологій можуть охоплювати різні види діяльності, пов'язані з використанням інформаційних ресурсів та мереж, і вони можуть включати в себе різні аспекти.

Національні та міжнародні нормативні акти та угоди, що стосуються кіберзлочинності, можуть включати визначення деяких конкретних кримінальних правопорушень, таких як несанкціонований доступ до комп'ютерних систем, крадіжка даних, атаки на інформаційну інфраструктуру тощо. Проте вони можуть бути недостатніми для врахування швидкого розвитку злочинності у сфері інформаційних технологій та нових її форм.

Крім того, в Україні і в інших країнах термін «кіберзлочинність» також часто асоціюється зі злочинністю в інтернеті та віртуальному просторі, оскільки багато кіберзлочинів відбуваються онлайн. Тим не менш, з розвитком інформаційних технологій випадки кіберзлочинності можуть мати реальні впливи на фізичний світ і суспільство загалом.

Варто зазначити, що проблематика забезпечення інформаційної безпеки в Україні та запобігання злочинності у сфері інформаційних технологій досліджується багатьма науковцями з різних галузей права, тобто має міждисциплінарний характер. Для визначення стану наукової розробленості розглянемо основні дослідження вчених цього питання.

Почнемо з того, що кримінальні правопорушення у сфері інформаційних технологій мають свою унікальну специфіку, яка відрізняє їх від традиційних кримінальних правопорушень, і ускладнює їх кримінологічний аналіз та наукове дослідження. Основними особливостями цифрових загроз і злочинності у сфері інформаційних технологій, які впливають на стан доктринального дослідження, включають: 1) новизна: історія злочинності у сфері інформаційних технологій є відносною новизною порівняно з історією традиційних кримінальних правопорушень. Це означає, що багато аспектів злочинності у сфері інформаційних технологій все ще досліджуються, і правові, кримінологічні та технічні аспекти цього явища продовжують еволюціонувати; 2) абстрактність: кримінальні правопорушення у сфері інформаційних технологій не обмежуються конкретним географічним регіоном, оскільки вони відбуваються в онлайн-середовищі. Це робить їх метафізичними або абстрактними, і визначення часу і місця вчинення кримінального правопорушення може бути вкрай складним; 3) використання технологій: кримінальні правопорушення у сфері інформаційних технологій зазвичай вимагають використання інформаційних ресурсів, технічних прийомів, алгоритмів і програмного забезпечення. Злочинці можуть використовувати ці засоби для доступу до комп’ютерів і мереж, крадіжки інформації тощо; 4) вплив на третіх осіб: кіберзлочинці можуть впливати на третіх осіб через інтернет, що робить кримінальне правопорушення більш анонімним і дистанційним. Це може ускладнити визначення злочинців і їх розслідування; 5) інтернет-посередники: багато кіберзлочинців використовують інтернет-посередників, такі як комп’ютери або сервери, для

здійснення атак. Це може ускладнити виявлення їхньої активності та ідентифікацію [15, с. 105].

Проте з розвитком злочинності у сфері інформаційних технологій це явище стало одним із основних напрямів дослідження у правничій науці.

Аналізуючи дисертаційні роботи щодо забезпечення інформаційної безпеки слід відмітити, що більшість з них стосується адміністративно-правового забезпечення інформаційної безпеки в Україні та її спрямованості на захист відповідають загрозам інформаційній безпеці. Однією з основних тез виступає те, що інформаційна безпека не обмежується лише заходами захисту, і важливо також враховувати прогнозування та аналіз нових трендів і розвитку кіберсуспільства.

Проте у роботах застосовано застарілий підхід, де спочатку аналізуються загрози, а потім формуються напрями їх запобігання. Такий підхід може бути недостатнім, оскільки інформаційна безпека потребує більш комплексного і системного підходу. Ретроспективний аналіз дійсно може мати обмежений корисний внесок у вирішення сучасних інформаційних викликів.

Сучасний підхід до інформаційної безпеки передбачає розгляд інформаційної безпеки як більш комплексного поняття, що включає не лише заходи захисту, але й аспекти прогнозування, запобігання загрозам, реагування на інциденти та відновлення після них. Це допомагає забезпечити більш ефективний та збалансований підхід до забезпечення інформаційної безпеки.

Важливою частиною сучасного підходу є також урахування та взаємодія з іншими сферами, такими як кіберзахист, кіберпрогнозування, розвиток нових технологій і заходи з підвищення кіберсвідомості серед громадян. Отже, підхід до інформаційної безпеки повинен бути гнучким, орієнтованим на майбутнє і комплексним, щоб відповідати сучасним інформаційним реаліям і викликам.

Відзначимо, що він презентований у підручнику «Інформаційна безпека (соціально-правові аспекти)». Тут розкриваються сутність, технології й засоби маніпулювання свідомістю, проведення інформаційних війн і спеціальних інформаційних операцій, історія та сучасний стан інформаційно-психологічного протиборства, особливості інформаційного впливу в терористичній діяльності та економічному протиборстві [190, с.150].

У дисертації Ю. Є. Максименко «Теоретико-правові засади забезпечення інформаційної безпеки України» складові інформаційної безпеки були виокремлені шляхом аналізу загроз національній безпеці в інформаційній сфері відповідно до Закону України «Про основи національної безпеки України». На думку Ю. Є. Максименко, інформаційна безпека становить систему, що складається з таких структурних елементів, як інформаційна безпека у сфері прав і свобод людини та громадянина, інформаційно-технічна і інформаційно-психологічна безпека [195, с.188].

Науковець зазначає, що кібербезпека стала невід'ємною частиною загальної інформаційної безпеки, оскільки включає в себе заходи для захисту інформаційних та технологічних ресурсів від цифрових загроз. Аналіз нормативно-правових актів у сфері кібербезпеки може вказувати на те, що більшість зусиль спрямовані на регулювання суспільних відносин у цьому напрямку з точки зору технічної інформаційної безпеки. Однак важливо також забезпечити, щоб права і свободи людини та громадянина залишалися захищеними в інформаційному просторі. Це вимагає розробки і вдосконалення нормативно-правових актів, які б враховували баланс між забезпеченням кібербезпеки та збереженням гарантованих прав і свобод людини. Правильний підхід полягає в тому, щоб розвивати інформаційну безпеку як комплексну систему, де технічні заходи поєднуються з правовими гарантіями прав та свобод громадян, а також із забезпеченням інформаційно-психологічної безпеки [195].

Ґрунтовною також є робота В. А. Ліпкана, Ю. Є. Максименко, В. М. Желіховського «Інформаційна безпека України в умовах євроінтеграції», в якій вперше наведено ознаки інформаційних війн, інформаційного протиборства, а також закладено засади до формування інформаційної та безпекової політики в безпековій сфері [189, с. 45]. У роботі основним є урахування стандартів Євросоюзу в формуванні інформаційного суспільства в Україні, що є досить суттєвим внеском у науку. Здійснення національних інтересів має бути центральним пріоритетом для будь-якої країни під час розвитку інформаційного суспільства. Проте важливо також враховувати міжнародний контекст та стандарти, особливо коли мова йде про кібербезпеку, яка має глобальний характер.

Урахування стандартів Євросоюзу може бути корисним в контексті гармонізації правил та підходів до кібербезпеки, що сприяє співпраці з іншими країнами та підвищенню загального рівня

безпеки в інтернеті. Проте важливо зберегти баланс між національними інтересами і міжнародними стандартами, щоб забезпечити національну безпеку та суверенітет, одночасно співпрацюючи з іншими країнами для спільного реагування на кіберзагрози.

У роботі «Систематизація інформаційного законодавства України» В. А. Ліпкан та В. А. Залізняк зазначають, що інформаційна безпека є важливою складовою для забезпечення стабільності та безпеки суспільства, оскільки вона впливає на різні сфери діяльності, включаючи економіку, політику, науку, технології, культуру та інші. Вчені слушно зауважують, що міждисциплінарний підхід до розуміння інформаційної безпеки дозволяє краще розкрити її сутність і враховувати її зв'язок з іншими аспектами сучасного життя. Оскільки інформаційні технології та процеси надзвичайно динамічні, важливо розглядати інформаційну безпеку як постійний інтегральний процес, який стосується як фізичних, так і інформаційних аспектів [188, с. 56].

На нашу думку, цей підхід дозволяє справедливо оцінювати загрози та ризики в інформаційній сфері і розробляти відповідні заходи для захисту інформації та забезпечення інформаційної безпеки на різних рівнях суспільства.

У сфері кібербезпеки та інформаційної безпеки зміни відбуваються настільки швидко, що чіткі та сталі визначення можуть швидко застаріти або не враховувати нові виклики і загрози. Тому інтегральний підхід та гнучкість визначення понять є більш адаптивними в умовах постійних трансформацій. Дослідження в галузі кібербезпеки та інформаційної безпеки має бути динамічним і відкритим для нових ідей та концепцій. Саме такий підхід дозволяє адаптуватися до нових загроз і розвитку технологій, а також ефективно захищати інформацію та інформаційні системи.

Продовжуючи аналіз наукових досліджень потрібно згадати роботу Т. В. Скубіної «Адміністративно-правове забезпечення інформаційної безпеки в органах державної фіскальної служби України», в якій напрями діяльності органів державної влади в сфері інформаційної безпеки, що стосуються оподаткування, є важливими для забезпечення ефективності та надійності податкової системи. Основні заходи і дії у цих напрямках допомагають забезпечити безпеку обробки та зберігання податкової інформації, попереджати податкові кримінальні правопорушення і шахрайство, а також сприяють підвищенню якості послуг для громадян і підприємств.

Доцільно розглянути кожний з цих напрямків, визначений авторкою, більш детально:

1. Правове регулювання суспільних відносин у сферах інформатизації та інформації – це основний фундамент для створення надійної інформаційної інфраструктури та правильного функціонування податкової системи.
2. Впровадження електронного документообігу та цифрового підпису дозволяє покращити ефективність обробки документів і забезпечити їх цілісність та автентичність.
3. Розвиток інформаційно-технічних засобів і систем сприяє покращенню роботи податкових органів та забезпечує їх можливість вчасно реагувати на податкові порушення.
4. Криптографічний і технічний захист інформації – це важливий елемент забезпечення конфіденційності та цілісності податкових даних.
5. Автоматизація та використання інформаційних систем допомагають податковим органам оптимізувати робочі процеси та підвищити їх ефективність.
6. Використання загальнодержавних довідково-інформаційних баз даних сприяє зручному та доступному доступу до необхідної інформації для податкових органів.
7. Оперативно-розшукова діяльність та співпраця з міжнародними організаціями у сфері інформатизації важливі для виявлення та припинення податкових порушень з міжнародними компонентами [294, с.123].

Важливими є висновки І. Р. Березовської, яка у дисертації «Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні» поділила загрози національним інтересам в інформаційній сфері на такі групи: 1) загрози діяльності влади щодо реалізації національних інтересів в інформаційній сфері; 2) загрози об’єктам національних інтересів в інформаційній сфері, які, своєю чергою, поділені на загрози: а) інформації (відомостям, повідомленням); б) інформаційній інфраструктурі; в) правовому статусу людини в інформаційній сфері [19, с.18].

Тобто, знову чітко бачимо кібербезпековий компонент, який вписується в систему інформаційної безпеки.

У роботі І. С. Стаценко-Сургучової «Організаційно-правові засади організаційно-аналітичної роботи в органах державної податкової служби України» досить важливою є теза про те, що

захист інформаційних ресурсів в органах державної податкової служби України є складовою більш широкого поняття інформаційної безпеки та умовою для її забезпечення. Згадане є важливим з огляду на ту обставину, що далі у монографії аналізуватимуться три основні напрями кібербезпекової політики, які виділив законодавець: кібербезпека, кіберзахист, кібероборона [300, с. 21].

Заслуговує на увагу і робота А. В. Туніка «Правові основи захисту персональних даних» [315, с. 212].

Зокрема, важливими є висновки автора щодо зарубіжного досвіду у сфері захисту персональних даних, в результаті якого робиться висновок, що у країнах ближнього зарубіжжя система захисту персональних даних здійснюється відповідно до закону типу Data Protection Act (Закон про захист даних), тоді як у європейських системах захисту персональних даних організуючим законодавчим центром стають два закони, що взаємодоповнюються – закон Data Protection Act і закон Information Freedom Act (закон про свободу інформації), які, як правило, розробляються і ухвалюються одночасно [315, с. 141].

Досить цікавими є пропозиції цього дослідника щодо застосування двох методів удосконалення системи захисту інформації про особу – реалістичного та ліберального. Метод реалістичного підходу передбачає збільшення безпеки всередині інформаційної системи, що є важливим, оскільки багато загроз виникають саме всередині системи через недоліки у програмному забезпеченні, недбалість персоналу та інші фактори. Створення нових внутрішніх мереж, моніторинг рівня інформаційної безпеки, пошук недоліків у програмному забезпеченні, зменшення відкритості доступу до персональних баз даних – це важливі кроки у підвищенні безпеки інформації. Метод ліберального підходу, з іншого боку, передбачає збільшення взаємозалежності щодо захисту персональних даних між країною і особою-власником персональних даних. Створення мережі спеціалізованих організацій і підписання спеціалізованих договорів може сприяти загальній безпеці інформації та захисту персональних даних. Лібералізація інформаційних стосунків може зробити процес обміну даними більш ефективним та зручним для користувачів [315, с. 178].

Отже, забезпечення інформаційної безпеки та захисту персональних даних – це складний процес, і комбінація реалістичного та

ліберального підходів може допомогти досягти більшої ефективності та надійності в цій сфері.

Важливим компонентом та джерельною базою виступають безпекові дослідження інформаційної політики, одним із яких є робота О. М. Яхно «Україна в сучасному геополітичному просторі (політико-медійний аспект)» [340, с.170], на думку якої рівень розвитку інформаційної складової тісно пов'язаний із безпекою держави: період становлення механізмів інформаційного суспільства є дуже небезпечним, оскільки країна може увійти у світові інфраструктури, не створивши при цьому механізмів захисту [340, с. 10].

Моделі інформаційної політики держави, які сформульовані О. М. Яхно, відображають різні підходи та стратегії, які може вибрати країна щодо управління інформаційним простором:

1. Інформаційна експансія: ця модель передбачає активну політику держави в інформаційному просторі, спрямовану на поширення свого впливу, інформаційної культури та ідентичності за межами своїх кордонів. Країна активно веде інформаційну пропаганду та намагається впливати на інформаційні процеси в інших країнах.

2. Відкриття інформаційного простору держави в обмін на допуск до інформаційних потоків інших країн та участь в їх формуванні: ця модель передбачає більш відкритий підхід до інформаційного простору, згоду на обмін інформацією та співпрацю з іншими країнами. Держава готова відкрити свій інформаційний простір для інших країн у обмін на доступ до їх інформаційних ресурсів.

3. Відкриття інформаційного простору, не беручи участі при цьому в світових інформаційних процесах: ця модель передбачає відкриття власного інформаційного простору для доступу громадян та іноземців, але при цьому держава не активно втручається в світові інформаційні процеси і не бере участі в формуванні світової інформаційної політики.

4. Відсутність особливої уваги до питання інформаційного суверенітету: ця модель передбачає байдужість держави до питань інформаційного суверенітету та відсутність активної політики в цьому напрямку.

У контексті євроінтеграційних процесів найбільш прийнятною для України, на думку О. М. Яхно, є друга модель [340, с. 9].

Не можемо погодитися з такою позицією через те, що відкриття інформаційного простору держави в обмін на допуск до інформаційних потоків інших країн не дало позитивного результату, а навпаки – ослабило державу в інформаційному плані, починаючи з 2014 року. Ми наголошуємо на важливості необмеженої залежності державної кіберполітики від зміни політичних влад, але науково обгрунтованих та сталих стратегічних напрямків, які сприяють досягненню національних інтересів. Це може бути важливим для створення стійкої кіберполітики, яка не зазнає значних змін при зміні влади. Також акцентуємо на необхідності захисту кіберпростору від зовнішніх загроз і забезпечення національної кібербезпеки. Це важливе завдання, особливо у зв'язку із зростанням кібератак та інших кіберзагроз. Формування і розвиток кібереліти та національної кібербезпеки мають допомогти забезпечити національну безпеку та інтереси України в кіберпросторі.

Проте управлінський та організаційний аспект є не менш важливими в контексті кібербезпеки та кіберполітики, і вони повинні бути ретельно розроблені та впроваджені, щоб забезпечити ефективний захист і керівництво в кіберпросторі.

Ще у 2006 році О. А. Яхно дуже чітко спрогнозувала появу так званої «гібридної війни», вказуючи на те, що в Україні існує баланс відносин у форматі «етнос-держава». Прогноз О. А. Яхно щодо появи «гібридної війни» та підкреслення важливості інформаційної складової у геополітичних стратегіях виявився дуже точним і важливим у контексті розвитку подій в Україні та світі. Гібридна війна включає в себе використання різних інструментів, таких як інформаційна пропаганда, дезінформація, кібератаки, психологічна війна, вплив на громадянське суспільство та інші, для досягнення політичних цілей [340, с. 5–8].

Ця стратегія набула особливої актуальності в умовах інформаційного суспільства, де інформація швидко поширюється і впливає на громадську думку та прийняття рішень. Тому важливо формувати та реалізовувати ефективні механізми для виявлення, запобігання та реагування на такі загрози.

У цьому контексті ґрунтовним є дослідження Д. В. Дубова «Політико-комунікативна безпека України у євроінтеграційному контексті», в якому автор, інтерпретуючи концепцією м'якої сили до розглядуваної ним тематики, запропонував концепцію м'якої десуверенізації [122, с. 165].

Цікавим є висновок Д. В. Дубова: «процес євроінтеграції характеризується поступовою втратою суверенітету держав, що відбувається на тлі поступового «одержавлення» самого ЄС. Розглянуто основні напрями здійснення цих процесів – федералізації в рамках ЄС, створення «євробюрократами» власного «апарату примусу» та спроби створення власне спільноєвропейської Конституції та спільних зовнішньополітичних інституцій, набуття ЄС «символьної» атрибутики, характерної для суверенних країн. Сформульовані три основні складові принадливого образу ЄС – фактор «забезпечення стабільності та безпеки», фактор доступу до «рогу достатку» та фактор «залучення до еліти» [122, с. 20].

Отже, висновки Д. В. Дубова підкреслюють важливість аналізу та реагування на вплив іноземних агентів та хакерських угруповань на кіберпростір і кіберкультуру країни. Зараз ця проблема є дуже актуальною, оскільки іноземні суб'єкти можуть впливати на громадську думку, політичні процеси та інші аспекти життя країни через інтернет і кіберпростір. Загрози інформаційної безпеки, пов'язані з іноземним впливом на кіберкультуру та кібернетичну активність, можуть мати серйозні наслідки для національної безпеки. Це може включати в себе спроби вплинути на вибори, поширення дезінформації, кібератаки та інші дії, спрямовані на зміну внутрішньої ситуації в країні.

З цими загрозами можна боротися шляхом підвищення кібербезпеки, обмеження доступу до критично важливої інформації, розвитку систем виявлення та реагування на кібератаки, а також зміцнення своєї кіберкультури та інформаційної грамотності суспільства.

Забезпечення кібербезпеки та формування різноманітних підходів до розроблення заходів її захисту можна знайти в роботах Є. Я. Прохоренко, О. О. Проскуріна. Н. Б. Новицької, А. М. Коломієць та інших [268, с. 67; 266, с. 76; 159, с. 46; 209, с. 35].

Дослідження В. М. Семіколенова «Мораль в інформаційному суспільстві» є важливим і актуальним в контексті сучасного світу. Інформаційне суспільство вносить значні зміни в наше сприйняття і розуміння моральних цінностей і норм. Аналіз ролі моральної рефлексії в протистоянні інформаційному маніпулюванню свідомістю дуже важливий, оскільки інформаційний простір, зокрема соціальні мережі і ЗМІ, може бути використаний для поширення дезінформації, фейкових новин та маніпуляцій з метою впливу

на громадську думку. Моральна рефлексія допомагає людям критично оцінювати інформацію і виробляти власні моральні позиції [287, с. 156].

Також важливо розглядати роль інформаційної еліти у формуванні моралі, оскільки вони можуть впливати на сприйняття моральних цінностей і норм в суспільстві. Глобалізація також має великий вплив на мораль, оскільки вона призводить до зміни культурних, етичних і моральних цінностей в різних частинах світу.

Зараз потрібно активно відшуковувати і проваджувати оновлені заходи забезпечення кібербезпеки в Україні з огляду на стрімке поширення цього явища, за яким не завжди встигають правоохоронні органи.

Саме тому право повинно бути не так регулятором, як стабілізатором цих відносин.

Зокрема, в свій роботі «Американський чинник в процесі інформаційної глобалізації» К. О. Данилишина прямо вказує на майже одноосібне панування США в сучасній системі міжнародних відносин і контролем цієї країни над усіма складовими світових інформаційних потоків і кібербезпекових складових. Підкреслення ролі США в сучасній системі міжнародних відносин і їх вплив на інформаційну сферу та кібербезпеку є важливими аспектами аналізу глобальної ситуації. США мають значний економічний, політичний і технологічний вплив у світі, і цей вплив розповсюджується і на сферу інформації та кібербезпеки [111, с. 4].

Інформаційна глобалізація дійсно зробила світ більш взаємозалежним і підвищила роль інформаційних потоків у міжнародних відносинах. У цьому контексті США, як лідери у багатьох сферах, можуть мати великий вплив на ці потоки і, відповідно, на кібербезпеку. Це стосується як цивільних аспектів, так і військової сфери.

Отже, досліджуючи питання щодо забезпечення інформаційної та кібербезпеки в Україні розглядалося на рівні дисертаційних та монографічних праць. Важливими в контексті нашої тематики є висновки вчених про необхідність оновлення системи захисту інформаційної безпеки та кібербезпеки, при цьому використовуючи сучасний методологічний інструментарій.

Окрім цього, проблемам впливу інформаційно-комунікаційних технологій на суспільне життя, інформаційній безпеці, кіберзлочинності та кібербезпеці присвячені роботи багатьох учених у

галузі кібернетики, інформатики, економіки та фінансів, цивілістики, кримінального права, кримінології, криміналістики та інших наук. Різні аспекти згадуваної проблематики розглядаються у роботах таких вітчизняних та зарубіжних учених, як Д. С. Азаров, Ю. М. Батурин, О. І. Бугера, В. В. Гостєв, М. В. Гуцалюк, М. А. Дем'янчук, В. М. Дрьомін, Д. В. Дубов, С. В. Кавун, О. В. Климчук, А. А. Комаров, А. П. Леонов, В. В. Лунєєв, В. В. Марков, Ю. М. Онищенко, К. С. Пивоварська, Н. А. Розенфельд, Т. Л. Тропіна, Д. М. Цехан, В. Т. Шатун та інших.

Існує багато різних термінів і понять, що використовуються для опису кримінальних правопорушень у сфері інформаційних технологій через широкий спектр дій та технологій, пов'язаних із цими протиправними діяннями. Використовуються такі терміни, як «кіберзлочинність», «комп'ютерна злочинність», «злочинність у сфері використання електронно-обчислювальних машин», «злочинність у сфері високих технологій», «злочинність у сфері інформаційних технологій», «злочини у сфері IT-технологій», «інформаційна злочинність», «hi-tech злочини» й інші.

Ці різні терміни можуть використовуватися в залежності від контексту та специфіки дослідження. Однак незалежно від термінології, вони всі вказують на категорію кримінальних правопорушень, пов'язаних із використанням комп'ютерів, мереж, інтернету і сучасних технологій для вчинення правопорушень.

Не маючи на меті визначення та розмежування усіх указаних понять, слід зазначити, що термін злочинність у сфері інформаційних технологій є універсальним та найбільш вдалим для використання у межах цього дослідження. Пояснюється це тим, що, по-перше, саме термін «кіберзлочинність» (cybercrime) отримав законодавче закріплення на міжнародному та вітчизняному рівнях. Це Конвенція Ради Європи «Про кіберзлочинність» [166], Закон України «Про основні засади забезпечення кібербезпеки України» [250].

Крім того, підтвердженням практичної поширеності як універсального терміну «кібер» є створення у 2015 р. Департаменту кіберполіції Національної поліції України [259]. Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної

політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність [252].

Варто зазначити, що у багатьох країнах світу діють спеціалізовані суб'єкти забезпечення кібербезпеки, які також у своїй назві використовують корінь «кібер» (cyber): наприклад, у США, Великій Британії та Німеччині – Національні центри кібербезпеки (National Cybersecurity Center, Nationales Cyber-Abwehrzentrum) і т.д.

В. М. Дрьомін, досліджуючи місце мережі Інтернет у механізмі інституціоналізації злочинності, звертає увагу на глобалізацію кіберзлочинності та її транснаціональний характер. Він зазначає: «комп'ютерні злочини небезпечні не тільки самі по собі, але й тим, що створюють умови для вчинення нових кримінальних правопорушень, розширюють сферу кримінальної дійсності та сприяють відтворенню злочинності, глобалізуючи її. Електронна комунікація може бути використана злочинцями для планування або координації практично усіх незаконних дій у будь-якій точці світу. Інтернет сприяє інституціоналізації неформальних соціальних практик, адже неформальні стандарти спілкування набувають глобальний та фактично неконтрольований характер» [122, с. 377].

Так, дослідження теоретичних аспектів кримінологічної характеристики злочинності у сфері інформаційних технологій знаходять своє відображення у працях численних зарубіжних і вітчизняних науковців. Зокрема, проблемні питання сучасної інтернет-злочинності вивчає О. В. Таволжанський. Стан і тенденції кіберзлочинності на міжнародному і національному рівнях стали предметом наукових доробків Н. В. Сметаніної. Роль психологічного портрету для превенції та розкриття кіберзлочинів у своїх працях висвітлює М. В. Карчевський. Криміналісти В. М. Шевчук та В. Ю. Шепітько досліджують аспект використання інформаційних технологій для встановлення особи злочинця. Запобігання корпоративним проявам кіберзлочинності висвітлює у своїх працях В. В. Пивоваров. Зарубіжні науковці Ш. Шольберг, Д. Паркер, С. Хантінгтон присвятили праці питанням кіберзлочинності у контексті міжнародно-правового регулювання, проблемам організованої злочинності в інтернет-просторі, а також розробленню методів протидії комп'ютерним кримінальним правопорушенням.

Відтак тема кіберзлочинності є відносно відомою і доволі розробленою в межах наук кримінального циклу, проте за умови

стрімкого розвитку суспільних інтернет-відносин і невпинного технологічного прогресу науковий доробок цього напряму потребує постійного і систематичного доопрацювання та актуалізації. Зокрема, зростає потреба у дослідженнях суто практичного спрямування, які надають власне трактування провідним аспектам кримінологічного аналізу кіберзлочинності, детально характеризуючи осіб, які вчиняють кіберзлочини [221, с. 354].

Одними з перших з вітчизняних дослідників, хто звернув увагу на загрози кіберзлочинності були П. Д. Біленчук та М. А. Зубань. На початку незалежності, 32 роки тому, коли комп'ютерами та, тим більше, мережею Інтернет у нашій країні мало хто користувався, вийшов навчальний посібник «Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти» [26, с. 72]. Під комп'ютерними злочинами запропоновано розуміти суспільно небезпечні дії або бездіяльність, що здійснюються з використанням сучасних технологій і засобів комп'ютерної техніки, з метою заподіяння шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадських організацій і громадян, а також правам особи [26, с. 6].

Погоджуємося із думкою В. А. Номоконова, який вказує, що явище кіберзлочинності включає в себе кримінальні правопорушення, вчинені у кіберпросторі. Він пише: «кіберзлочинність – це сукупність злочинів, що вчиняються у кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних» [211, с. 48].

Порівнюючи близькі за змістом категорії «кіберзлочинність» та «комп'ютерна злочинність», В. А. Номоконов та Т. Л. Тропіна зазначають, що ці терміни дуже близькі за змістом, але не синонімічні. Поняття «кіберзлочинність» ширше, ніж «комп'ютерна злочинність», і більш точно відображає природу такого явища, як злочинність в інформаційному просторі [211, с. 87].

М. О. Кравцова у рамках дисертаційного дослідження під кіберзлочинністю пропонує розуміти соціально-правовий феномен, що проявляється у забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних

машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [173, с. 7].

Дещо дискусійні визначення кіберзлочинів та кіберзлочинності формулює С. А. Буяджи: «кіберзлочинами є найбільш небезпечні кіберправопорушення, вчинення яких на різних стадіях безпосередньо пов'язане із використанням комп'ютерної техніки через комп'ютерні системи, або із комп'ютерними системами, та за які чинним законодавством передбачено кримінальну відповідальність» [75]. «Кіберзлочинність – сукупність окреслених кримінальним законом вчинків, вчинених на тій чи іншій території або щодо об'єктів, розташованих на ній за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп'ютерні системи, комп'ютерні мережі і комп'ютерні дані» [75].

В. М. Бутузов пропонує розглядати комп'ютерну злочинність як підсистему злочинності у сфері новітніх інформаційних технологій, що пов'язана із протиправним використанням комп'ютерних технологій автоматизованої обробки інформації. Зазначається, що кримінальні правопорушення у сфері новітніх інформаційних технологій – вчинені умисно або з необережності суспільно небезпечні діяння (дії або бездіяльність), що посягають на відносини у сфері обробки інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, надання та отримання телекомунікаційних послуг, проведення електронних розрахунків [72, с. 303].

Беручи за основу теоретичний аналіз наукових напрацювань інших учених, а також законодавче трактування кіберзлочинності, можемо надати таке визначення цього поняття.

Поняття кіберзлочинності включає в себе важливі аспекти та характеристики цього явища. Воно враховує кримінальні правопорушення, які вчиняються в кіберпросторі, зокрема шляхом доступу до комп'ютерних даних, мереж, а також телекомунікаційних мереж, включаючи Інтернет і мобільний зв'язок. Враховування широкого спектру технологій і мереж підкреслює актуальність кіберзлочинності у сучасному інформаційному суспільстві.

На думку Г. М. Чернишова, кіберзлочинність – це кримінальні правопорушення, вчинені з використанням та/або проти кіберпростору. Кіберзлочинність – злочини, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення [333].

М. О. Кравцова у дисертаційному дослідженні розглядає явище кіберзлочинності та запобігання цих кримінальних правопорушень органами внутрішніх справ [173, с.16].

На рівні дисертаційних робіт окремі аспекти зазначеної проблематики вивчалися М. В. Карчевським «Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)» (2003 р.) [146, с. 175], «Кримінально-правова охорона інформаційної безпеки України» (2013 р.) [147, с. 230], О. Е. Радутним «Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю» (2002 р.) [272], Н. А. Розенфельд «Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» (2003 р.) [278, с. 176], Д. О. Ричкою «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [277, с.200].

У 2005 році вийшов науково-практичний коментар за редакцією А. А. Музики та Д. С. Азарова «Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення», який присвячено кримінально-правовому аналізу складів злочинів, передбачених статтями розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» особливої частини Кримінального кодексу України, та суміжних з ними посягань.

Однією з найновіших наукових досліджень є дисертація С. В. Шапочки «Запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж» (2018 р.), у якій репрезентовано власну класифікацію шахрайства, що вчиняється з використанням комп'ютерних мереж, визначаються детермінанти та ступінь його латентності [334, с. 160].

Зокрема, В. В. Ткачук вказує на об'єктивну обумовленість і потребу інформатизації освіти як єдиного засобу швидкісної передачі інформації. Інтенсифікації навчально-виховного процесу, нарощування обсягу знань, підвищення ефективності контролю успішності учнів та здобувачів вищої освіти, розширення інтелектуальних

можливостей учасників навчально-виховного процесу, удосконалення управління закладом освіти та системою освіти [311, с. 24].

Отже, розробка концепції права кібернетичної безпеки є важливим завданням в сучасному інформаційному суспільстві. Основною метою цієї концепції є створення системи правового регулювання, яка б забезпечувала ефективний захист від кіберзлочинності та зберігала кібербезпеку. Це включає в себе розробку правових норм, нормативів, стандартів, а також уніфікованих протоколів та процедур для захисту інформаційних ресурсів.

Концепція права кібернетичної безпеки повинна також враховувати етичні, соціокультурні, інституціональні та технологічні аспекти. Вона має бути динамічною і адаптивною до змін у кіберзагрозах та технологічному прогресі.

Формування кібернетичної ідентичності є важливою частиною цієї концепції, оскільки вона сприяє розумінню і прийняттю цифрових технологій та їх впливу на суспільство. Правова база повинна враховувати інтереси громадян, держави та підприємств у цифровому середовищі та забезпечувати їхню кібербезпеку.

Розробка такої концепції вимагає співпраці науковців, юристів, технічних експертів та інших зацікавлених сторін, щоб створити цілісну і ефективну систему правового регулювання кібербезпеки [116, с. 412].

На основі вивчення наукових джерел щодо забезпечення інформаційної безпеки в Україні та запобігання злочинності у цій сфері можемо виокремити напрями наукових досліджень:

1) дослідження загальних засад інформаційної безпеки в Україні (В. А. Ліпкан, В. А. Залізняк, Ю. Є. Максименко, В. М. Желіховський, В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк, А. В. Тунік, Д. В. Дубов);

2) вивчення правового забезпечення інформаційної безпеки в Україні (І. С. Стаценко-Сургучова, І. Р. Березовська, Т. В. Скубіна);

3) безпекові дослідження (О. М. Яхно);

4) загально-правові питання забезпечення кібербезпеки (Є. Я. Прохоренко, О. О. Проскурін, Н. Б. Новицька, А. М. Коломієць);

5) теоретичні аспекти кримінологічної характеристики кіберзлочинності (Ш. Шольберг, Д. Паркер, С. Хантінгтон, О. В. Таволжанський, Н. В. Сметаніна, М. В. Карчевський, В. В. Пивоваров,

В. А. Номоконов та Т. Л. Тропіна, В. М. Бутузов, С. А. Буяджи, Г. М. Чернишов, М. О. Кравцова, О. Е. Радутний, С. В. Шапочка);

6) криміналістичні аспекти розслідування (В. М. Шевчук та В. Ю. Шепітько, В. С. Бабійчук).

1.3. Генезис дослідження проблематики злочинності у сфері інформаційних технологій

Серез кримінологів побутує думка про те, що злочинність у сфері інформаційних технологій – явище досить нове. Проте через поширеність і суспільну небезпечність вказаного виду злочинності необхідно дослідити його витоки для можливості аналізу дій злочинців у майбутньому.

Отже, історичні витоки та причини злочинності у сфері інформаційних технологій, формування системи запобігання цьому виду злочинності науковці почали досліджувати відносно недавно. До таких вчених можна віднести О. С. Алавердова, Ю. М. Батуріна, П. Д. Біленчука, А. В. Войцехівського, М. Д. Діхтяренка, К. Ю. Ісмайлова, С. М. Круля, Є. Д. Скулиша, Т. Л. Тропіної, Б. Х. Толеубекова та ін. Проте на сьогодні не є достатньо дослідженими питання щодо історії становлення вказаного виду злочинності, і, на нашу думку, це питання є важливим і актуальним, оскільки вивчення причин і умов розповсюдження злочинності у сфері інформаційних технологій дасть змогу сформувати цілісну і ефективну систему запобігання їх вчиненню.

На сьогодні виділяють такі етапи розвитку кіберзлочинності:

1 етап – поява кіберзлочинності та субкультури хакерів.

2 етап – розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності та національних груп хакерів.

3 етап – набуття кіберзлочинністю транснаціонального характеру, поява кібертероризму та міжнародних угруповань хакерів в усіх сферах кіберзлочинності.

4 етап – використання мережі Інтернет в політичних цілях, виникнення таких явищ, як Інтернет-страйк та Інтернет-війна, цілеспрямоване використання кібератак проти урядів окремих держав [115].

С. А. Буяджи у дисертаційному дослідженні на тему: «Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект», значну увагу приділив генезису правового регулювання

боротьби з кіберзлочинністю в світі та Україні. Внаслідок аналізу правової доктрини автором виділені чотири етапи процесу розвитку явища кіберзлочинності.

До першого етапу автор відносить підготовчий етап який охоплює кінець 60-х років – початок 70-х років XX століття, що є початковим моментом вчинення злочинів із використанням електронних обчислювальних машин.

Другий етап – розповсюдження кіберзлочинності, який охоплює початок 70-х років XX століття – 1986 рік) – ознаменувався початком появи хакерів та їх організованих груп, а завершився із прийняттям першого в історії нормативно-правового акту, присвяченого кіберзлочинам та першого в історії арешту хакера;

Третій етап автор визначає як етап транснаціональних кіберзлочинів та кібертероризму (1994 рік – початок XXI століття).

Четвертий етап – сучасний етап кіберзлочинності (XXI століття) – етап появи нових форм комп'ютерних злочинів.

На нашу думку, автор слушно доходить до висновку, що генезис розвитку кіберзлочинності та генезис правового регулювання боротьби з кіберзлочинністю не можна ототожнювати. Кіберзлочинність розвивається у відповідності з еволюцією новітніх технологій, тому на сьогодні є сферою, яка постійно на крок попереду її нормативно-правового регулювання [75].

Дану позицію підтримують Є. В. Коваленко та О. В. Плетньов, які, звертаючи увагу на те, що кіберзлочинність має дуже високий потенціал розвитку та підвищення своєї негативної ефективності, зазначають невідповідність швидкості розвитку засобів кримінально протиправної діяльності у кіберпросторі швидкості законодавчого врегулювання та впровадження тих або інших засобів запобігання такій діяльності [154, с. 59].

І. В. Діордіца, досліджуючи питання щодо змісту кіберзагроз на сучасному етапі, доходить висновку про те, що неналежне правове регулювання в національному кібернетичному просторі України призводить до низки негативних явищ, які створюють реальні та потенційні загрози кібернетичній безпеці. У зв'язку з чим, автор акцентує увагу на необхідності розроблення науково обґрунтованої державної політики в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її

сферах, захисту від інформаційних загроз і реалізації права на отримання достовірної інформації [117, с. 101].

Як ми уже відмічали, з появою та розповсюдженням інформаційних технологій у всі сфери життя суспільства почала розвиватись й кіберзлочинність. Щодня злочинці, використовуючи інформаційні технології в кримінально протиправних цілях, вчиняють все більшу кількість кримінальних правопорушень, ідучи на «крок вперед» від працівників правоохоронних органів. Необхідність оновлення системи запобігання злочинності у сфері інформаційних технологій спонукає до якнайшвидшого пошуку найкращого шляху для її вдосконалення, який має включати в себе створення відповідних комп'ютерних систем і технологій, з високим рівнем безпеки в мережі та відповідної нормативно-правової бази, яка буде регулювати сповна це питання та встановлювати належну міру покарання за вчинення кримінальних правопорушень цього виду.

Варто зазначити, що кіберзлочинність, порівняно з традиційними видами злочинності в Україні (вбивства, корисливі кримінальні правопорушення тощо), є відносно новим явищем і найбільшою загрозою XXI століття водночас, адже інформаційні технології також є способом вчинення багатьох традиційних кримінальних правопорушень. Злочинці використовують інтернет-технології через їх основні характеристики: глобальність, анонімність користувачів, охоплення різної за віком та географічним положенням аудиторії. Саме це дає можливість особам отримати кримінально протиправний результат та уникнути відповідальності.

Виникнення кіберзлочинності пов'язується із поширенням так званого віртуального простору, який містить інформацію про осіб, події, явища, процеси тощо, зашифровані у математичному, символьному чи будь-якому іншому вигляді [115, с. 2]. Тому зрозуміло, що кіберзлочинність є відносно новим видом кримінально протиправної діяльності, який потребує спеціальних навичок і знань та специфіка якої полягає у тому, що технічні можливості для його вчинення з'явились порівняно нещодавно, а отже варто звернутись до історичних передумов його появи та розвитку.

Виникнення терміну «комп'ютерна злочинність» хронологічно пов'язується із початком 60-х років минулого століття, коли були виявлені перші випадки кримінальних правопорушень, вчинених з використанням електронних обчислювальних машин [353, с. 5]. «Батьківщиною» цього виду злочинності вважаються США, де у

1945 р. було створено першу електронну обчислювальну машину, одну із ранніх форм комп'ютерів, яка використовувалась для розшифровування німецьких військових кодів, а згодом й з іншою метою. Те саме має місце і в наш час, коли комп'ютери та мережеві системи використовуються, в першу чергу, для вирішення завдань інформаційної безпеки, а вже згодом для інших локальних цілей [123, с. 133]. Тому не випадково, що вчинення першого в історії комп'ютерного кримінального правопорушення відбулось у Міннесоті, де у 1966 році було зафіксовано перший випадок використання електронної обчислювальної машини як інструмента при пограбуванні банку [269, с. 79]. У подальшому поява та розповсюдження комп'ютерної техніки та передових технологій постало у якості реальної загрози національній безпеці держав. Це питання почало турбувати науковців. Наприклад, починаючи з 1958 року, дані правової статистики Стенфордського дослідницького інституту так характеризують види «комп'ютерних» злочинів XX століття: 1) випадки пошкодження і розкрадання комп'ютерного устаткування, розкрадання інформації; 2) шахрайство або розкрадання грошей, здійснені із застосуванням комп'ютерів; 3) несанкціоноване використання комп'ютерів або розкрадання машинного часу [123, с. 133]. Тобто, на той момент на науковому рівні вже було сформовано чітке розуміння появи нового виду злочинності та про необхідність її подолання. Не зважаючи на оперативну реакцію з боку науковців, все свідчить про те, що держави світу не були готовими до виникнення таких загроз.

На противагу цього потрібно зазначити, що становлення та розвиток кіберзлочинності не можна відокремлювати від інформаційної революції, тому початком її відліку доцільно вважати шістдесяті роки минулого століття. Саме у 1962 р. професор Джон Лікрайдер, опублікував свою концепцію розповсюдженої комп'ютерної мережі «Galactic Network» [312, с. 304].

Головним припущенням цієї концепції було те, що в майбутньому з'явиться глобальна мережа, приєднатися до якої зможе кожен охочий, а також у тому, що ця мережа у своїй діяльності може об'єднувати усі комп'ютерні системи світу. Окрім загальної думки, вчений детально охарактеризував принципи глобальної мережі, які стали основоположними для мережі Інтернет [88].

Оскільки така ідея та її втілення були новим та надзвичайно цікавим процесом, який міг спростити життя мільйонів людей у всьому світі, то результат не змусив себе чекати: скоро з'явилась перша мережа комп'ютерів ARPANet (Advanced Research Projects Agency Network), створена на замовлення Міністерства оборони США. Головна мета цієї розробки полягала у тому, щоб створити розподілену систему, яка б не мала чіткого центру, і складалася б з взаємозамінних частин. Спочатку ARPANet мала у складі чотири комп'ютери, розташованих у великих дослідницьких центрах. Головним завдання мережі була передача інформації та електронне листування, тому жодні серйозні елементи, що обмежували б доступ, в її структурі не існували, оскільки тоді ніхто навіть і не припускав появи злочинців у мережі. Цей недолік надалі успадкує і мережа Інтернет, що в подальшому призведе до явища «анархізм». Непродуманість аспектів безпеки і юридичного контролю при розробці технічних принципів мережі у майбутньому буде наслідком широкого розповсюдження кіберзлочинності.

У 1970-х роках з'являються перші комп'ютерні злочинці, яких почали називати «хакерами». Хто ж точно був першим хакером, сказати важко, проте у переважній більшості літературних джерел про хакерів та для хакерів, як першого професійного кіберзлочинця згадують Джона Дрейпера, який також проводив першу спеціалізацію хакерів, – фрікери (phreaker), скорочене від телефонний хакер (phone haker). У рядах фрікерів того часу були усім відомі Стів Возняк та Стів Джобс, які в майбутньому стали засновниками «Apple Computers». Саме вони налагодили виробництво пристроїв для злому мереж у домашніх умовах. І цей час доцільно вважати початком розвитку кіберзлочинності [100, с. 296].

Отже, комп'ютерна злочинність зародилася вже в ранній епосі використання комп'ютерів і цей період можна розглядати як початковий етап в її розвитку. Важливо враховувати, що з розвитком технологій і доступністю комп'ютерів та мереж комп'ютерна злочинність стала значно розповсюдженою та складною.

На відміну від інших видів злочинності, які можуть бути більш традиційними, комп'ютерні кримінальні правопорушення часто складно виявити і відслідковувати, оскільки вони вчиняються в електронному середовищі, а зловмисники можуть використовувати анонімність і шифрування для приховування своєї діяльності. Тому

розвиток правових інструментів для боротьби з кіберзлочинністю стає все більше актуальним завданням.

Отже, основними рисами першого, початкового етапу розвитку кіберзлочинності є:

1) перші випадки кримінальних правопорушень, вчинених з використанням електронних обчислювальних машин, свідчать про початок розвитку цього явища та зростання інтересу до комп'ютерної і мережевої діяльності як засобу для вчинення кримінальних правопорушень;

2) формування організованих злочинних груп, які використовували свої знання для незаконного збагачення та порушення встановленого порядку, свідчить про еволюцію цього явища від окремих випадків до організованої діяльності;

3) на цьому етапі відсутність ефективних інструментів правового регулювання боротьби з кіберзлочинністю стала значущим обмеженням у запобіганні цим кримінальним правопорушенням;

4) існувала відсутність випадків покарання комп'ютерних злочинців за їх протиправну діяльність, оскільки правова база для цього була недостатньо розвиненою.

Варто відзначити, що вперше основні ознаки комп'ютерних кримінальних правопорушень були сформульовані Американською асоціацією адвокатів у Далласі в 1979 році та визначили ключові аспекти цього виду злочинності. Ці ознаки допомагають розуміти характер і мотивацію злочинців, а також встановлювати фактичні обставини вчинення кіберзлочинів. Вони також стали основою для подальшого розвитку правового регулювання в сфері кібербезпеки:

1) використання або спроба використання комп'ютера для одержання грошей, власності чи послуг шляхом обману або підробки. Ця ознака вказує на фінансовий аспект комп'ютерних кримінальних правопорушень, де злочинці намагаються здійснити шахрайські дії за допомогою комп'ютерних ресурсів;

2) навмисна несанкціонована дія з метою зміни, пошкодження, знищення або викрадення комп'ютерних систем або даних. Ця ознака вказує на аспект завдання шкоди комп'ютерним системам або інформації, що може мати важливий вплив на кримінально протиправну діяільність.

3) навмисне несанкціоноване порушення зв'язку між комп'ютерами або мережами комп'ютерів. Ця ознака вказує на спроби перешкодити нормальному функціонуванню комп'ютерних систем

або перервати зв'язок між ними [269, с. 76]. У 1979 році комп'ютерні кримінальні правопорушення представляли собою абсолютно нове явище, особливо для колишнього СРСР та інших країн, де законодавство та правопорядок не були готові до регулювання цього типу злочинності. В цей період багато країн почали створювати відповідне законодавство та стратегії боротьби з комп'ютерною злочинністю, але вони стали більш актуальними з розвитком і поширенням інформаційних технологій та Інтернету.

Потрібно звернути увагу на те, що у цей період злочинність у сфері інформаційних технологій стає глобальним явищем. У 1983 році в США відбулась історична подія – перший арешт кіберзлочинця, про який стало відомо громадськості. Групою підлітків було здійснено Інтернет-злом близько 60 комп'ютерів. Після арешту один із учасників дав свідчення, тож усі інші члени організованої групи отримали умовний термін покарання [192, с. 86]. Ця подія є важливою в контексті нашого дослідження із таких причин: арешт та покарання комп'ютерних злочинців вказують на те, що на той момент у деяких країнах вже існували правові норми, які визнавали комп'ютерну злочинність і надавали поліції та правопорядковим органам повноваження для її запобігання. Умовний строк може свідчити про те, що деякі кримінальні правопорушення можуть бути розглянуті як менш суспільно небезпечні порівняно з іншими видами кримінально протиправних діянь.

Наступна вагома подія, яка має безпосереднє відношення до генезису правового регулювання боротьби з кіберзлочинністю в світі, відбулась у 1986 році також у США – було прийнято перший в історії комп'ютерний закон «The Computer Fraud and Abuse Act». Прийняття цього закону стало важливим кроком у розвитку правового регулювання комп'ютерних кримінальних правопорушень і кібербезпеки. Цей закон визначив основні норми, які стосуються неавторизованого доступу до комп'ютерних систем і отримання секретної військової інформації. Також він визначив та захистив певні види несекретної інформації, включаючи інформацію фінансових установ, державних установ та міжнародних організацій. Цей закон став важливим прецедентом у створенні законодавства, спрямованого на боротьбу з комп'ютерною злочинністю та забезпечення кібербезпеки. Він визначив, що такі дії є протиправними і можуть бути покарані за законом [379].

Важливими наслідками вступу в дію цього нормативно-правового акту є: 1) було заборонено розповсюдження вірусів, які на той момент набули значного поширення; 2) у 1986 році вперше заарештовано хакера – Ллойда Бланкеншипа [103, с. 97]. Саме з прийняттям цього нормативного акту науковці пов'язують завершення другого етапу розвитку злочинності у сфері інформаційних технологій.

Отже, етап розповсюдження кіберзлочинності (початок 70-х років XX століття – 1986 рік) характеризується наявністю таких основних рис: 1) чітке формування концепції комп'ютерних кримінальних правопорушень на науковому рівні; 2) поширення кіберзлочинності на територію Радянського Союзу, до складу якого входила і Україна; 3) відбувся перший в історії арешт кіберзлочинця, про який стало відомо громадськості – це є свідченням існування на той момент основ законодавства про кіберзлочинність; 4) прийняття в Сполучених Штатах Америки першого у світовій історії «комп'ютерного» закону.

Наступна важлива подія в історії розвитку кіберзлочинності – це так звана «справа Володимира Льовіна», учасника організованої злочинної групи, яка, використовуючи Інтернет, спробувала перевести грошові кошти із рахунків банку на особисті рахунки. До цього моменту вчинення жодного великого міжнародного кримінального правопорушення не розголошувалось громадськості, тож така справа вважається першою, віднесеною до категорії транснаціональних мережевих комп'ютерних кримінальних правопорушень [97, с. 35].

Цей історичний період вчені пропонують називати етапом транснаціональних кіберзлочинів та кібертероризму, оскільки наступний щабель розвитку комп'ютерної злочинності пов'язується з її виходом на міжнародний рівень та появи ознак цілеспрямованого застосування терору у великих масштабах [75].

Загалом у 80-х роках прослідковується значне збільшення кількості комп'ютерних атак. Якщо в 1988 р. було тільки шість звернень із цього приводу до центру Інтернет-безпеки CERT, який почав діяти у 1988 р., то в 1989 р. число звернень налічувало 132, а в 1990 – вже 252 [98, с. 118].

Поява нових спеціалізацій у сфері Інтернет-злочинів та консолідація злочинців у великі групи вказує на те, що кіберзлочинність стає більш організованою та вдосконаленою. Цей етап

розвитку кіберзлочинності можна розглядати як природний відгук на зростання обсягів інформації та використання Інтернету як засобу для вчинення різних кримінальних правопорушень.

У 1984 р. Фред Коен опублікував повідомлення про відкриття перших шкідливих комп'ютерних програм, які здатні до саморозмноження, і визначив їх терміном «комп'ютерний вірус». Також він створив програму, яка ілюструвала спосіб зараження одного комп'ютера іншим [172, с. 321].

Загалом поняття «кібертероризм» викликає різні точки зору серед експертів і вчених. Це обговорювана тема і визначення та характеристики кібертероризму можуть варіюватися в залежності від контексту та точки зору авторів. Деякі дослідники вважають, що кібертероризм – це використання комп'ютерних атак і інших кіберзлочинів з метою тероризму, наприклад, для атак на критичну інфраструктуру або для поширення деструктивних програм.

У той же час інші дослідники вважають, що термін «кібертероризм» може бути перебільшеним і що існує більше загроз від кібератак, які використовуються для розвідки, шпигунства або дестабілізації, ніж для прямого тероризму.

Незважаючи на різні точки зору, важливо визнавати, що кіберзагрози і кібератаки можуть мати серйозні наслідки для критичної інфраструктури, господарства і національної безпеки країн. Тому боротьба з кіберзлочинами і підвищення кібербезпеки залишаються важливими завданнями для держав і міжнародних спільнот [87, с. 45].

Слід відмітити, що злочинність у сфері інформаційних технологій у кінці XX ст. значно поширилась і відповідно змінився віковий ценз злочинців цієї категорії.

У 1998 р. 12-річний хакер зламав комп'ютерну систему, яка координувала водоспуск дамби Теодора Рузвельта в Арізоні. Небезпека його незаконних дій полягала у тому, що у разі відкриття зливних воріт дамби вода могла б затопити міста Темп і Месе, загальна чисельність населення яких нараховувала близько 1 млн. жителів. Оцінка цього діяння стала підґрунтям для появи таких термінів як «Інтернет-тероризм», «комп'ютерний тероризм», «кібертероризм». До того ж, це вказало на те, що найбільш уразливою до кібератак є сама мережа Інтернет, адже усі її ключові елементи доступні з будь-якої точки світу [214].

Розвиток кіберзлочинності, зокрема кібертероризму та кібершахрайства, справді набуває транснаціонального характеру завдяки здатності кіберзлочинців та кібертерористів діяти в онлайн-середовищі з будь-якого куточка світу. Це дозволяє їм здійснювати кібератаки та інші кримінальні дії на міжнародному рівні, не маючи фізичного присутності у країнах-жертвах.

Помилки або необережність фахівців, а також вразливості в інфраструктурі та програмному забезпеченні можуть призвести до серйозних проблем в кібербезпеці. Так, у 1997 р. помилка співробітника «Network solutions» стала наслідком того, що сайти, назви яких мали в закінченні «.net» та «.com» стали недоступними. Що свідчить про те, що збій в роботі усієї глобальної мережі стався через неуважність однієї людини. Це підкреслює важливість навчання та підвищення компетентності у сфері кібербезпеки, а також постійного моніторингу та оновлення заходів щодо захисту інформації і кіберінфраструктури [214].

Використання кібератак у політичній сфері стало серйозною загрозою, і такі атаки часто отримують назву «кіберполітичних атак». Ці атаки можуть бути спрямовані на вплив на політичну ситуацію, вибори, голосування та інші події, що стосуються політики.

Одним з прикладів такої атаки є Distributed Denial of Service (DDoS) атаки на веб-сайти політичних кампаній або новинних ресурсів. У результаті DDoS-атаки, велика кількість запитів надходить на сервер, перевантажуючи його та призводячи до недоступності веб-сайту для користувачів.

Також важливо визначити поняття дезінформації (disinformation) та маніпуляції інформацією (information manipulation) як інструментів політичного впливу у кіберпросторі. Злочинці можуть розповсюджувати фальшиву інформацію, провокувати конфлікти, створювати негативне враження про певних політиків чи партії з метою вплинути на громадську думку та рішення виборців.

Слід згадати, що на сьогодні практично будь-який політичний або збройний конфлікт йде поряд з організованою протидією у мережі Інтернет. Зокрема, у 2005 р. Відбулася низка кібератак, приводом для яких був шкільний підручник з історії, який був виданий в Японії, та у своєму змісті змінював зміст подій в Китаї в 1930–1940-х рр. XX ст. Якщо детально, то в ньому «замовчувалися» військові кримінальні правопорушення японських військ під час

вторгнення. Такі кібератаки здійснювалися на веб-сайти державних органів, органів місцевого самоврядування, а також великих підприємств. Вони були синхронними, що свідчить про надзвичайну майстерність злочинців. Науковці припускали, що такі атаки були організовані саме для досягнення політичних цілей [222, с. 134].

Вчені стверджують, що наразі відбувається останній етап розвитку кіберзлочинності – етап появи нових форм комп'ютерних кримінальних правопорушень. Як пише В. Б. Дзюндзюк, серед них варто відзначити такі: 1) Інтернет-війна – уперше групи комп'ютерних активістів, засуджуючи військові дії Югославії та НАТО, здійснювали злом урядових комп'ютерів та поширювали антивоєнну Інтернет-пропаганду; 2) Інтернет-страйк – групова діяльність, яка призводить до перевантаження Інтернет-сайту на неможливість його відвідування іншими користувачами тощо [115]. Очевидно, що такий перелік нових форм є далеко невичерпним, проте основна мета його відзначення – продемонструвати, що питання правового регулювання боротьби з кіберзлочинністю в світі потребує постійної еволюції і вдосконалення, адже комп'ютерні злочинці постійно змінюють напрямки та методи своєї діяльності. Тож, основними ознаками сучасного етапу є: 1) еволюція кіберзлочинності, виникнення її нових форм; 2) спроби законодавців адекватно реагувати на дані зміни.

Отже, внаслідок аналізу правової доктрини, науковцями виділено такі етапи процесу розвитку явища кіберзлочинності:

1. Підготовчий етап (початок 60-х років – початок 70-х років XX століття) – початковим моментом варто вважати перші випадки кримінальних правопорушень, вчинених із використанням електронних обчислювальних машин, наприкінці комп'ютерні зловмисники вже представляли із себе організовані злочинні групи, які використовували власні знання для незаконного збагачення та порушення встановленого порядку;

2. Етап розповсюдження кіберзлочинності (початок 70-х років XX століття – 1986 рік) – початком варто вважати появу хакерів та їх організованих груп, а завершення пов'язати із прийняттям першого в історії нормативно-правового акту, присвяченого кіберзлочинам та першого в історії арешту хакера;

3. Етап транснаціональних кіберзлочинів та кібертероризму (1994 рік – початок XXI століття) – початковий момент цього етапу пов'язується із «справою Володимира Льовіна», першим великим

міжнародним транснаціональним мережевим комп'ютерним злочином, а кінцева дата обрана умовно – нами здійснено її прив'язку до початку нового століття, у якому не відбулось вагомих історичних подій у розвитку кібертероризму, проте у якому відбувається планомірна еволюція комп'ютерної злочинності;

4. Сучасний етап кіберзлочинності (XXI століття) – етап появи нових форм комп'ютерних кримінальних правопорушень [75].

Отже, можемо зробити висновок, що розвиток кіберзлочинності і правового регулювання її боротьби є двома відокремленими, але взаємопов'язаними процесами. Кіберзлочинність зростає і еволюціонує разом з розвитком технологій, і боротьба з нею повинна постійно адаптуватися до нових загроз і викликів, які вона створює.

Важливо враховувати, що недоцільність або відсутність правового регулювання може призвести до беззаконня та безкарності у сфері кіберзлочинності, що має потенціал призвести до серйозних наслідків. Тому розвиток адекватних і ефективних законодавчих інструментів та міжнародного співробітництва в цій галузі є критично важливими аспектами у боротьбі з кіберзлочинністю.

З огляду на історичний розвиток запобігання злочинності у сфері інформаційних технологій у світі доцільно розглянути відповідний розвиток в Україні.

На сьогодні Україна перебуває на початковому етапі боротьби з комп'ютерною злочинністю. Аналіз історії розвитку цього явища в інших країнах та встановлення співвідношення зі світовим досвідом може допомогти створити більш ефективну та відповідну реакцію на кіберзагрози та злочинність.

Історія розвитку кіберзлочинності та правового регулювання в Україні та багатьох інших країнах світу демонструє, як важливо бути пильними та адаптувати законодавство до змін у технологіях та сучасних кіберзагроз. Справа «вінницького переказу» 1998 року є типовим прикладом ситуації, коли законодавство не було готове відповісти на виклики, які поставила кіберзлочинність [160, с. 89]. Проте цей випадок так і не увійшов до історії комп'ютерної злочинності України, оскільки через недосконалість вітчизняного законодавства не був віднесений до кіберзлочинів.

На щастя, уряди багатьох країн, включаючи Україну, в останні роки більше уваги приділяють кібербезпеці та боротьбі з кіберзлочинністю. Проаналізувавши інциденти, подібні до «вінницького переказу», і вивчивши найкращий досвід із світової практики,

Україна може розробити та впровадити більш сучасні та ефективні закони, спрямовані на боротьбу з кіберзлочинністю.

З часом Україна, як і багато інших країн, почала докладати більше зусиль для боротьби з кіберзлочинністю. Розвиток інформаційних технологій і зростання інтернет-залежності вимагають активного втручання і змін у законодавстві та правопорядку, щоб забезпечити захист від кіберзагроз.

Вважаємо, що поштовхом для стрімкої еволюції стали взяті Україною зобов'язання щодо інтеграції у міжнародну та світову спільноту, наприклад прийняті згідно до Програми інтеграції України в Європейський Союз [262]. Так, Розділ 13 Програми було присвячено інформаційному суспільству.

У 2001 році було прийнято Кримінальний кодекс України, у якому: 1) окремі види кіберзлочинів було виділено у Розділі XVI Особливої частини «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж – статті 361, 362 та 363; 2) Розділом V Особливої частини «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину – статті 163, 176, 177; 3) Розділом VII «Злочини у сфері господарської діяльності» – стаття 200 [179]. Значення прийняття Кримінального кодексу України можна виразити такими аспектами: 1) незаконна діяльність у кіберпросторі була вперше визнана злочином на рівні вітчизняного законодавства; 2) за кіберзлочини було встановлено конкретні санкції; 3) прийняття Кодексу послужило поштовхом для настання наступного етапу генезису правового регулювання боротьби з кіберзлочинністю – етапу прийняття вітчизняного законодавства про боротьбу із кіберзлочинністю.

Паралельно із цим процесом, актуальність проблеми кібер-безпеки було зокрема висвітлено в Указах Президента: «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14.07.2000 р. № 891 [242], «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000 [243], «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001 [236] тощо. Поряд з тим, відмічаємо, що навіть з наявністю відповідного

нормативного регулювання цього питання кіберзлочинність в Україні стрімко зростала.

У 2003 році було прийнято Закон України «Про основи національної безпеки» від 19.06.2003 № 964-IV, у якому, зокрема, були закріплені поняття «комп'ютерна злочинність» та «комп'ютерний тероризм» та їх віднесення до основних реальних та потенційних загроз національній безпеці України [245].

Ратифікація Конвенції про кіберзлочинність і імплементація її положень у вітчизняне законодавство України є кроком у правильному напрямку для зміцнення кібербезпеки та боротьби з кіберзлочинністю в країні. Це свідчить про готовність України враховувати міжнародний досвід та норми для захисту від кіберзагроз та кримінальних правопорушень.

З іншого боку, важливо також забезпечити ефективну реалізацію цих норм у практиці та здійснювати постійне удосконалення законодавства про кіберзлочинність відповідно до змін у технологіях та сучасних загрозах. Забезпечення кібербезпеки вимагає постійного оновлення та адаптації правових інструментів до нових реалій.

Відзначимо, що на сучасному етапі розвиток злочинності у сфері інформаційних технологій в нашій державі ще не досяг значних масштабів. Серед суттєвих кібератак варто виділити нещодавнє застосування невідомими зловмисниками вірусу «Petya.A» проти значної кількості стратегічних об'єктів нашої держави. Зокрема, відомо, що одним із шляхів потрапляння вірусу до комп'ютерних мереж було оновлення бухгалтерського програмного забезпечення «M.E.Doc» [152].

Аналіз судової практики засвідчує, що найбільш поширеними кримінальними правопорушеннями у сфері інформаційних технологій є несанкціоноване втручання в роботу автоматизованих систем і різноманітні шахрайства з використанням електронно-обчислювальної техніки.

Щодо прикладів вітчизняної судової практики, то 21 січня 2016 року Стрийським міськрайонним судом Львівської області було розглянуто справу щодо несанкціонованого втручання в роботу автоматизованих систем, зокрема банкомату. Зловмисники встановили два несанкціоновані пристрої, які мають умовну назву «накладка на банкомат» і призначені для прихованого розміщення на банкоматі з метою отримання інформації з магнітних стрічок банківських карт

користувачів та здійснення відеофіксації виконання ними операцій на цифровій клавіатурі банкомату, що призвело до проникнення в автоматизовану систему вказаного банкомату та витоку інформації 45 клієнтів вказаної вище банківської установи, на яких містилась інформація з магнітних стрічок карт та пінкодів клієнтів банку [83]. Оскільки статтею 361 Кримінального кодексу України передбачено відповідальність за незаконне втручання в роботу електронних обчислювальних машин, зробимо висновок, що вітчизняний законодавець адекватно реагує на подібні загрози.

Поширеними на сьогодні є випадки шахрайства з використанням електронно-обчислювальної техніки. Так, 22.05.2017 року Першотравневим районним судом міста Чернівці було винесено вирок у справі № 725/85/17 щодо вчинення із корисливих мотивів ряду дій, спрямованих на підготовку та реалізацію шахрайства. Зловмисниця розмістила на Інтернет-сайті оголошення про здачу в оренду кімнати, достовірно знаючи, що житла за вказаною адресою у неї не має та наміру здавати кімнату в оренду вона не мала. Особа повідомила потерпілому завідомо неправдиву інформацію, та отримала грошову суму у якості завдатку [82]. У цьому випадку кримінальне правопорушення кваліфікувалося за статтею 190 Кримінального кодексу України. Тут законодавець не відокремив окремо шахрайство за допомогою електронно-обчислювальної техніки, проте у даному випадку все ж основоположну роль відіграє факт заволодіння чужим майном шляхом обману. Тому, незважаючи на наявні ознаки кіберзлочину, подібні правопорушення варто кваліфікувати як шахрайство.

Наступним прикладом є вирок Ленінського райсуду міста Кіровограда (нині м. Кропивницький) у справі № 405/1660/14-к. Зловмиснику було пред’явлено обвинувачення у вчиненні розповсюдження відеопродукції порнографічного характеру за допомогою веб-сайту «http://vk.com» [81]. Не зважаючи на те, що це кримінальне правопорушення було кваліфіковано за статтями 300 та 301 Кримінального кодексу України, а саме ввезення, виготовлення, збут і розповсюдження порнографічних предметів та творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, це порушення все ж має чіткі ознаки кіберзлочинів, адже його вчинення пов’язується із Всесвітньою мережею.

Віднедавна в Реєстрі судових рішень з'являються цікаві судові рішення, які стосуються вітчизняної кібербезпеки. Зокрема, заслуговує на увагу рішення Комунарського районного суду м. Запоріжжя від 10.03.2020 р. у справі № 333/714/20. Суть справи полягала в тому, що обвинувачений, використовуючи комп'ютерну техніку, здійснив несанкціоноване втручання до особистого кабінету потерпілого й отримав доступ до його облікового запису у відомій онлайн-грі «World of Tanks». Після цього обвинувачений отримав доступ до ігрового акаунта «World of Tanks», який належав потерпілому, та продав його невстановленій особі через Інтернет.

На думку суду, указані дії містили склад кримінального правопорушення, передбаченого ч. 1 ст. 361 Кримінального кодексу України: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. З огляду на це суд присудив особі, яка визнана винною у здійсненні шахрайських дій щодо отримання доступу до чужого ігрового акаунта, штраф у розмірі 10200 грн.

Особливо ці кримінальні правопорушення поширюються сьогодні, в умовах воєнного стану. Кіберзлочинність зросла в декілька разів, адже країна-агресор дуже часто вчиняє несанкціоноване втручання в роботу автоматизованих систем.

Про використання в умовах воєнних дій інформаційних технологій у кримінально протиправних цілях російською федерацією відомо вже давно. Така діяльність посилилась у зв'язку з повномасштабним вторгненням країни-агресора на територію України. Використання фейкових профілів у соцмережах, втручання у діяльність урядових порталів, сайтів державних органів, поширення російської пропаганди та агресії росії проти України – це не весь перелік кримінальних правопорушень у сфері інформаційних технологій, які вчиняє ця держава. За даними американського видання «Вашингтон пост», ще у 2014 російська військова розвідка створила більше 30 псевдо-українських груп і акаунтів у соціальних мережах, а також 25 «провідних англомовних» видань. Видаючи себе за пересічних українців, працівники головного розвідувального управління вигадували новини та поширювали коментарі, щоб

налаштувати проросійських громадян проти протестувальників [384]. Отже, можемо стверджувати про початок нового етапу розвитку злочинності у сфері інформаційних технологій, яких характеризується широким використанням засобів масової інформації у викривленні правдивої інформації, поширенні кібершахрайства та кібертероризму.

На основі цього можемо зробити висновок, що хоча злочинність у сфері інформаційних технологій є відносно новим видом злочинності, вона завдає значної матеріальної шкоди, і з моменту свого виникнення пройшла 5 етапів розвитку в Україні:

1) поява такого явища як злочинність у сфері інформаційних технологій та формування ідей та субкультури хакерів;

2) становлення злочинності у сфері інформаційних технологій як міжнародного виду злочинності; виникнення злочинних угрупувань хакерів, які спеціалізуються на вчиненні кримінальних правопорушень у різних країнах;

3) злочинність у сфері інформаційних технологій стає транснаціональною;

4) використання мережі Інтернет для досягнення політичної мети, поява а також використання кібератак проти урядів окремих держав;

5) активне використання інформаційних технологій під час війни, що супроводжується широким залученням засобів масової інформації задля дезінформації населення, поширенні кібершахрайства та кібертероризму [39].

Отже, зараз Україна активно рухається у напрямку підвищення кібербезпеки та правового регулювання цієї сфери, а також інтеграції з міжнародними стандартами та практиками. Ратифікація міжнародних правових актів та відповідність європейським стандартам є важливими кроками у зміцненні кібербезпеки та боротьбі з кіберзлочинністю. Збільшення усвідомлення загрози кібертероризму є дуже важливим, і відповідні заходи та політика мають бути спрямовані на запобігання таким загрозам та реагування на них.

Окрім цього, відмітимо ключові аспекти сучасного стану правового регулювання боротьби з кіберзлочинністю в Україні. Перехід до міжнародних стандартів та збільшення уваги до кібербезпеки та боротьби з кіберзлочинністю є позитивними кроками для захисту інформаційної інфраструктури та забезпечення інформаційної безпеки у країні. Зростання усвідомлення загрози кібертероризму

важливо для вчасного виявлення та запобігання подібним атакам. Належне правове регулювання кіберзагроз, які є найбільш поширеними в Україні, також є критично важливим для захисту інтересів країни та її громадян у кіберпросторі. Продовження роботи над удосконаленням правового регулювання, співпраця з міжнародними партнерами та постійний моніторинг кіберзагроз допоможуть Україні підвищити рівень кібербезпеки та ефективно боротися з кіберзлочинами.

Дослідження генезису правового регулювання боротьби зі злочинністю у сфері інформаційних технологій в Україні дозволяє виділити його такі етапи:

1. Початковий етап (1991 рік – кінець XX ст.) – прийняття базових нормативно-правових актів щодо забезпечення інформаційної безпеки, встановленню кримінальної відповідальності за кіберзлочини увага не приділялась

2. Напрацювання і прийняття нормативної бази щодо боротьби з кіберзлочинністю (2001 рік – 2011 рік) – прийняття Кримінального кодексу України, у нормах якого незаконна діяльність у кіберпросторі була вперше визнана кримінальним правопорушенням, а за кіберзлочини було встановлено конкретні санкції. Окрім цього, вперше у законодавстві визначено поняття «комп'ютерна злочинність» та «комп'ютерний тероризм»;

3. Етап відповідності правового регулювання боротьби з кіберзлочинністю існуючим загрозам (2011 рік – до 2021 рік) – внесення змін до законодавства, в тому числі, кримінального, щодо виконання вимог євроінтеграційного курсу України та у зв'язку з існуючими загрозами (вірус «Petya.A» тощо).

5. Новий етап (2021 рік – до сьогодні) – пов'язаний зі збройною агресією російської федерації в Україні та відкриттям другого фронту – інформаційного.

1.4. Методологія дослідження злочинності у сфері інформаційних технологій

Аналізуючи методологію дослідження злочинності у сфері інформаційних технологій звернемо увагу на складність та багатоплановість вивчення цього явища. Дійсно, ця галузь вимагає використання різноманітних методологій та підходів для розуміння та аналізу її складних аспектів [309, с. 248].

До основних аспектів методології дослідження злочинності у сфері інформаційних технологій можна віднести:

1) мультидисциплінарний підхід: дослідження кіберзлочинності вимагає співпраці між різними галузями науки та індустрією, включаючи правознавців, комп'ютерних фахівців, психологів, соціологів і багатьох інших. Мультидисциплінарний підхід дозволяє більш повно розуміти і аналізувати кіберзлочинність.

2) вивчення технологій: посилення злочинності у сфері інформаційних технологій часто пов'язане з використанням новітніх технологій. Дослідники повинні слідкувати за останнім розвитком у сфері інформаційних технологій та кібербезпеки.

3) збір та аналіз даних: збір і аналіз великих обсягів даних може допомогти виявити патерни та тренди в злочинності у сфері інформаційних технологій. Методи аналізу даних, такі як машинне навчання і аналіз великих даних, стають все більш важливими в цій галузі.

4) етичні аспекти: врахування етичних аспектів дослідження кіберзлочинності, таких як приватність і безпека даних, також має велике значення.

5) правова складова: аналіз правового регулювання і кримінального переслідування злочинності у сфері інформаційних технологій є важливою складовою дослідження.

6) соціальні аспекти: розуміння соціальних аспектів злочинності у сфері інформаційних технологій, включаючи мотиви та наслідки кіберзлочинців, також є важливим.

7) методи попередження і реагування: розробка методів та стратегій для попередження та реагування на злочинність у сфері інформаційних технологій також є важливою частиною дослідження.

Сучасна Україна перебуває на стадії формування і розвитку нового типу суспільних відносин, визнаного на світовому рівні «інформаційним суспільством», який, на думку зарубіжних фахівців, є третьою хвилею розвитку людства, що формується на основі аграрного та індустріального суспільства.

Наука кримінального права до цього часу не оперувала терміном «інформаційне суспільство», не приділяла достатньо уваги переосмисленню підходів убезпечення притаманних саме йому нових суспільних відносин від суспільно небезпечних посягань. У КК України та у теорії кримінального права суспільно небезпечні

діяння, які виникали у інформаційному суспільстві, відображені ситуативно, відповідно до найгострішой необхідності (ст.198-1 КК України 1960 р. [179], Розділ XVI Особливої частини КК України 2001 р. [177]. До цього часу не вбачаються кримінально-правовою наукою потреби убезпечення від посягань інформаційного простору, у якому відбуваються такі посягання, та дистанційних комунікацій, завдяки яким у інформаційному суспільстві здійснюються не лише суспільні відносини, а й суспільно небезпечні посягання на них.

Необхідність сприйняття інформаційного суспільства наукою і практикою кримінального права диктує потребу осмислення його основних чинників кримінально-правового забезпечення інформаційного суспільства і подальшої її реалізації у відповідному кримінально-правовому законодавстві. В. К. Грищук указує, що «безспірним методологічним підходом до вироблення кримінальної політики має бути широке поєднання соціологічних і кримінологічних методів, що дає можливість з'ясувати: а) які суспільні заходи слід застосовувати для нейтралізації суспільно небезпечного діяння; б) застосування яких суто правових (або не правових) засобів у даному випадку є найбільш раціональним; в) з'ясувати можливості комплексного застосування правових і не правових засобів; г) у разі визнання за доцільне застосувати кримінально-правові засоби встановити їх оптимальний режим» [105, с. 159].

Методологія дослідження, як його логічна організація, повинна складатися з констатації предмета та об'єкта дослідження, аргументації структури дослідження, визначення основних підходів у здійсненні, обранні засобів і методів, необхідних для його реалізації, а також іншої аргументації щодо основних інституцій, які входять у зазначені категорії.

Методологія такого дослідження становить комплекс засобів і прийомів пізнання [276, с. 21], спрямованих на визначення головної мети дослідження: комплексне міжгалузеве вивчення сучасного стану та перспектив розвитку кримінально-правового забезпечення інформаційного суспільства в Україні, предмета дослідження, підходів до визначення основних понять, які ґрунтуються на принципах об'єктивності та обґрунтованості юридичного пізнання, всезагальних, загальних і спеціально-юридичних методах наукового пізнання, і нерозривно пов'язана зі структурою дослідження.

Тому структура дослідження обумовлена необхідністю послідовного і логічного розкриття виокремлених у дисертації завдань. Вона

обумовлюється необхідністю забезпечення поступовості й послідовності під час здійснення детального аналізу сучасного стану кримінально-правового забезпечення інформаційного суспільства, визначення основних напрямів його розвитку та розробкою шляхів його удосконалення.

Методологія дослідження, яка охоплює обрання та визначення методів дослідження, безпосередньо впливає на побудову дослідження, оскільки правильна послідовність і належне застосування методів наукового пізнання обумовлює об'єктивність, логіку, неупередженість, правдивість і повноту дослідження всієї теоретичної та емпіричної бази. Методологія роботи обрана з огляду на об'єкт і предмет дослідження, оскільки метод вивчення будь-яких явищ повинен бути спрямований на специфіку предмета вивчення [186, с. 10].

Для комплексних досліджень із кримінального права об'єкт і предмет яких потребує сприйняття з точки зору низки наук, або є міжгалузевим за суттю, характерне застосування насамперед діалектико-матеріалістичного методу пізнання та сучасної теорії пізнання соціальних і правових явищ, які ґрунтуються на комплексі загальних філософських і спеціально-юридичних методів дослідження. Обумовлено найширше застосування філософських методів дослідження у цій дисертації, адже, як стверджує А. Лой, методологія сучасних соціальних наук немислима без філософії права, філософії політики, етики, аксіології та ін. [193, с. 37].

Водночас у процесі дослідження широко має використовуватися і загальнофілософський синергетичний метод, досі не популярний у правовій доктрині. Синергетичний метод наукового пізнання, що полягає у вивченні процесів самоорганізації та виникнення, підтримання, стійкості і розпаду структур різної природи на міждисциплінарному рівні, не може оминати міжгалузеві дослідження новоутворень, до яких, зокрема, належать суспільні відносини у інформаційному суспільстві. Так, сучасна філософія розуміє під синергетикою сучасну теорію самоорганізації, нове світобачення, що пов'язується з дослідженням феноменів самоорганізації, нелінійності та нерівномірності, глобальної еволюції, вивченням процесів становлення «порядку через хаос». Саме такий процес має сприяти убезпеченню суспільних відносин від хаотичних суспільно небезпечних виявів у інформаційному просторі, які в більшості сучасна кримінально-правова наука не помічає.

Використання синергетичного методу пізнання стає необхідним за здійснення комплексного дослідження кризових суспільних відносин, які існують у всіх сферах, водночас, фактично, не мають єдиного або навіть окресленого, ані теоретичного, ані практичного підходу до визначення, бачення, вирішення. Така потреба акцентується філософами саме щодо правової науки (державно-правової) [200, с.141].

Відтак, незважаючи на те, що синергетика виникла як методологічний напрям дослідження природничих наук, синергетичний напрям доцільний під час здійснення міжгалузевого пошуку за виконання правового дослідження. На користь такої доцільності слід навести думку А. Машкова: «Основна проблема парадигми науки XXI століття, – це доказ нею своєї власної універсальності. В контексті юридичної науки це означає наявність задачі обґрунтувати, що синергетична методологія придатна до досліджень державно-правової дійсності» [200, с. 143–144].

Зокрема, застосування синергетичного методу наукового пізнання необхідне для виявлення та оцінки соціальної цінності та ролі у сучасних суспільних відносинах основних ресурсів і соціальних цінностей інформаційного суспільства, їх соціальних, філософських, економічних, правових та кримінально-правових характеристик з метою виявлення основних об’єктів кримінально-правового забезпечення та, відповідно, формування завдань кримінально-правового забезпечення інформаційного суспільства, визначення сучасних об’єктів кримінально-правової охорони, необхідних напрямів національного та міжнародного кримінально-правового забезпечення та оцінки соціальної обумовленості криміналізації в інформаційному суспільстві. Також зазначений метод необхідний для кримінально-правової оцінки, зокрема, спілкування як природної потреби людини, яка досі не визнана правовою категорією, проте є ключовим фактором у розвитку громадянського сектору інформаційного суспільства; у дослідженні явищ впливів на свідомість різних видів, походження й оцінки їх суспільної небезпечності у інформаційному суспільстві, потреби криміналізації тощо.

Квінтесенцією правового і кримінально-правового розуміння інформаційного суспільства повинна стати специфічна, притаманна інформаційному суспільстві структура суспільних відносин і смисл предметів та цінностей, які зумовлюють утворення таких відносин,

виводять на новий рівень суспільні відносини нової доби розвитку людства. Установлення таких особливостей інформаційного суспільства може вважатися об'єктивним лише у процесі міжгалузевого дослідження цього феномена, концепцій його розвитку та прогнозів динаміки суспільних відносин у ньому, а також уразливих від суспільно небезпечних посягань основних складових такого суспільства.

Злочинність у сфері інформаційних технологій і її запобігання у її поєднанні динамізму та статичності, мінливість, структурованість, багатоплановість зумовлюють і відповідну структуру методології її дослідження, що складається з таких складових частин: домінуючого світогляду, типу наукового мислення, філософських засад, наукових парадигм, методологічних підходів та наукових методів.

Для висвітлення методологічних особливостей та можливостей дослідження злочинності у сфері інформаційних технологій доцільно зупинитись на характеристиці найбільш важливого пізнавального інструментарію, що складає фундамент окремих методик осмислення безпекової сфери, яким є сукупність найбільш ефективних та загальновизнаних у правознавстві методологічних підходів.

Варто звернути увагу на те, що дослідники, які займаються дослідженням злочинності у сфері інформаційних технологій, застосовують різні методологічні підходи в залежності від поставлених завдань та предмету дослідження. Найбільш поширеними методологічними підходами, які можуть бути використані в дослідженні злочинності у сфері інформаційних технологій, є:

Діяльнісний підхід: цей підхід спрямований на вивчення діяльності суб'єктів злочинності у сфері інформаційних технологій, їх мотивів і методів. Він допомагає розуміти, як самі злочинці діють та як можна розробити стратегії для їх виявлення та запобігання.

Системний підхід: цей підхід допомагає розглядати злочиність у сфері інформаційних технологій як складну систему, де різні елементи (злочинці, жертви, засоби тощо) взаємодіють між собою. Аналіз системних взаємозв'язків допомагає зрозуміти, як ця система функціонує та як можна впливати на її роботу.

Аксіологічний підхід: цей підхід спрямований на вивчення цінностей, які лежать в основі дій суб'єктів злочинності у сфері інформаційних технологій. Він допомагає розуміти моральні

аспекти злочинності та визначати, які цінності порушуються через кіберзлочини.

Функціональний підхід: цей підхід досліджує функції, які виконують інформаційні технології у сфері кіберзлочинності. Він допомагає розуміти, які можливості надають інформаційні технології для здійснення кримінально протирпавних дій та як ці можливості можна обмежити або використовувати в цілях захисту.

Порівняльно-правовий підхід: цей підхід полягає в порівнянні правових систем різних країн у контексті боротьби зі злочинністю у сфері інформаційних технологій. Він допомагає зрозуміти, які правові рішення ефективніше за інші та як можна використовувати кращі практики з інших країн.

Кожен з цих методологічних підходів може бути корисним для вивчення певних аспектів кіберзлочинності, і дослідники можуть використовувати їх в комбінації для отримання більш повного уявлення про цей складний явище.

Зокрема, діяльнісний підхід базується на засадах «теорії діяльності», використовується в різних соціально-гуманітарних науках, у його межах діяльність інтерпретується як пояснюючий принцип, парадигма, теоретична модель та метод наукових досліджень, що дають можливість розглянути навколишній світ як прояв, форму, умову, результат цілеспрямованого впливу людини та суспільства [108, с. 30–39].

Ваша характеристика діяльнісного підходу до дослідження злочинності у сфері інформаційних технологій добре відображає основні принципи цього підходу. Діяльнісний підхід акцентує увагу на цілеспрямованій діяльності суб’єктів, які здійснюють дії в сфері інформаційних технологій. Досліджуючи цю діяльність, дослідники можуть спрямовувати свої зусилля на досягнення певних цілей, таких як підвищення рівня безпеки в суспільстві та державі.

Діяльнісний підхід також враховує конкретно-історичні та соціально-культурні умови, в яких здійснюється діяльність. Це важливо, оскільки контекст може значно впливати на рівень злочинності в цій сфері. Наприклад, швидкий розвиток інформаційних технологій може створювати нові можливості для злочинців, а соціокультурні аспекти можуть визначати, які цінності і моральні норми домінують в даному суспільстві.

Крім того, діяльнісний підхід враховує, що безпека інформаційних технологій може бути важливою як для суспільства, так і для

окремих осіб. Деякі суб'єкти можуть діяти з метою захисту власної інформації, в той час як інші можуть вчиняти кримінальні правопорушення з метою завдання шкоди іншим. Таким чином, діяльнісний підхід враховує різні мотивації та інтереси суб'єктів в цій сфері.

Засоби для забезпечення безпеки інформаційних технологій також можуть бути різноманітними, оскільки вони повинні відповідати конкретним потребам і умовам. Це можуть бути технічні заходи, правові норми, етичні норми, а також інші способи забезпечення безпеки. Загалом, діяльнісний підхід дозволяє більш комплексно розглядати проблеми злочинності у сфері інформаційних технологій та розробляти стратегії для їх запобігання та виявлення.

Таким чином, діяльнісний підхід не виключає, а, навпаки, передбачає необхідність та доцільність використання інших методів – системного, структурного, функціонального, статистичного, а також психологічних, конкретно-соціологічних та інших, і може бути застосований до різних правових динамічних інформаційної безпеки, таких як: структура (склад) діяльності; засоби здійснення; гарантії; нормативна основа; функціональне значення; соціальна роль; середовище здійснення; віднесеність до певного виду або роду; виділення типологічних ознак; ефективність; законність (правомірність); режим здійснення; механізм здійснення [109, с. 4–5; 6].

Крім діяльнісного, фундаментальним методологічним підходом дослідження є системний підхід, який дозволяє розглянути запобігання злочинності у сфері інформаційних технологій як певну систему і як елемент (підсистему) державного управління, державної діяльності.

Системний підхід може мати різні визначення та інтерпретації в залежності від контексту і дисципліни. Він використовується в різних наукових галузях та сферах досліджень для аналізу та розуміння складних явищ та процесів.

Системний підхід може включати такі аспекти:

1) інтеграція та синтез: він допомагає об'єднувати та аналізувати різні аспекти або компоненти явища або системи, щоб побачити їх взаємозв'язок та вплив одних на інші. Це дає можливість отримати комплексне розуміння об'єкта дослідження.

2) адекватність об'єкта: системний підхід вимагає, щоб система була органічним цілим, тобто включала в себе взаємозв'язані

компоненти та функціонувала як єдність. Це допомагає уникнути довільності в визначенні систем та забезпечує їх адекватність дослідженню.

3) процедури та методики: системний підхід включає в себе конкретні методики та процедури, які використовуються для аналізу та розробки системних рішень. Це може включати математичні моделі, аналіз потоків, аналіз взаємозв'язків, симуляції тощо.

4) вибір оптимального рішення: системний підхід допомагає розглядати різні варіанти виконання завдання та вибирати оптимальний варіант на основі аналізу взаємодії між компонентами системи та їх впливу на цілісність.

5) врахування взаємодії: системний підхід покликаний допомогти у розумінні, як компоненти системи взаємодіють між собою та впливають на загальну динаміку системи. Він дозволяє розглядати систему як цілісну єдність.

Варто зазначити, що поняття системи, як і системного підходу, формувалося поступово, в міру того, як наука і практика опановували різні типи, види і форми цілісних об'єднань предметів і явищ. Реалізація системного підходу здійснюється у двох напрямах: пізнавальному і конструктивному (використовується під час створення систем) [129, с. 39].

У контексті нашого дослідження системний підхід використовувався у таких двох ключових напрямах:

1) описовий напрям: у цьому напрямку застосування системного підходу дозволяє проводити аналіз та опис державної політики у сфері безпеки з точки зору її складових, функцій, ролі в суспільстві та взаємодії з іншими системами і субсистемами. Це допомагає зрозуміти, як державна політика впливає на безпеку, ідентифікувати потенційні проблеми та ризики, а також розвивати стратегії для покращення цієї політики.

2) напрям проєктування: у цьому напрямку системний підхід використовується для розробки та проектування державної політики у сфері безпеки в конкретних умовах. Він дозволяє враховувати різні аспекти політики, такі як мета, завдання, ресурси, методи та інші фактори, що впливають на її успішність. Цей напрямок сприяє розробці ефективних та адаптивних стратегій безпеки.

Зазначимо, що використання системного підходу в дослідженні та розробці заходів запобігання злочинності у сфері інформаційних технологій допомагає зрозуміти складність цього питання та

враховувати взаємозв'язки між різними аспектами. Це сприяє раціональному прийняттю рішень та покращенню ефективності політики з питань безпеки.

Відповідно до напряму дослідження системний підхід реалізується на основі певної сукупності принципів:

1) принцип остаточної (глобальної, генеральної) мети: цей принцип вказує на необхідність чіткого визначення головної мети системи безпеки, яка може бути світовою, національною, регіональною або специфічною для певної суспільної групи або окремої особи. Глобальна мета системи повинна бути визначена так, щоб сприяти досягненню цілей безпеки на всіх рівнях.

2) принцип єдності, зв'язаності і модульності: цей принцип наголошує на тому, що система безпеки повинна розглядатися як єдина глобальна система, яка включає в себе численні взаємодіючі складові частини. Важливо розуміти, як ці частини взаємодіють між собою та як ця взаємодія впливає на систему в цілому.

3) принцип ієрархії: цей принцип відображає існуючу ієрархічну структуру системи безпеки, де різні органи та організації мають свої ролі та функції. Він підкреслює, що державна політика у сфері безпеки базується на ієрархічному розподілі функцій та повноважень між різними суб'єктами системи.

4) принцип функціональності: цей принцип вказує на те, що система безпеки повинна виконувати конкретні функції та завдання, які визначаються її метою та цілями. Важливо розуміти, які функції системи є ключовими для досягнення її мети та як вони можуть змінюватися з часом.

5) принцип розвитку: цей принцип наголошує на необхідності постійного розвитку та модернізації системи безпеки, оскільки загрози та вимоги змінюються з часом. Система повинна бути готовою адаптуватися до нових умов та викликів.

6) принцип децентралізації: Цей принцип вказує на тенденцію передачі функцій та повноважень у галузі безпеки на регіональний та місцевий рівні в рамках процесу децентралізації. Він враховує особливості регіональних та місцевих умов та потреб у забезпеченні безпеки.

7) принцип невизначеності: цей принцип відзначає, що система безпеки повинна бути готовою до невизначеності та непередбачуваних ситуацій. Вона повинна мати механізми для реагування на

нові та еволюційні загрози, навіть якщо вони не були передбачені на попередніх етапах планування.

Даний підхід дав можливість дослідити як саме явище запобігання злочинності, так і власне безпекову ситуацію як об'єкт впливу державної політики в єдності їх складових елементів; можливість визначити роль та місце окремих елементів державної політики; можливість визначити певні особливості їх взаємозв'язків та взаємодії.

Ще одним методом дослідження злочинності у сфері використання інформаційних технологій є функціональний підхід до дослідження цього явища, який підкреслює важливість розуміння ролі та функцій різних елементів системи інформаційної безпеки. Основні принципи цього підходу вказують на важливі аспекти аналізу:

1) єдність цілого: він наголошує на необхідності узгодженого функціонування всіх елементів інформаційної безпеки. Це важливо для забезпечення ефективності та уникнення дублювання функцій різних організацій.

2) універсальність: цей підхід вказує на те, що функції правоохоронних органів у вказаній вище сфері можуть бути різними, залежно від конкретних умов і загроз. Він підкреслює необхідність адаптації функцій до конкретних викликів і ситуацій.

3) необхідність: принцип необхідності допомагає визначити, які саме заходи запобігання є обов'язковими і які можуть бути вторинними або непотрібними в конкретних умовах.

4) порівняльно-правовий підхід дозволяє аналізувати запобігання злочинності у сфері інформаційних технологій з урахуванням різних аспектів та порівнювати її з іншими системами або правовими моделями. Це допомагає виявляти подібності і відмінності, а також зрозуміти, які підходи та рішення можуть бути корисними для вдосконалення таких заходів.

Також доцільно звернути особливу увагу на методи порівняльного аналізу, які можуть бути використані для дослідження різних аспектів правових явищ. Кожен з цих методів має свої особливості і може бути корисним у різних контекстах дослідження. Розглянемо деякі з них більш детально:

1) конфронтативний метод: цей метод спрямований на вивчення схожостей і розбіжностей між правовими явищами. Він дозволяє

виявити спільні аспекти та відмінності в правових системах або політиках безпеки різних країн чи регіонів.

2) контрастивний метод: він, навпаки, акцентується на вивченні розбіжностей між правовими явищами. Цей метод допомагає виділити основні відмінності між двома або більше об'єктами аналізу та визначити, як ці розбіжності впливають на результати чи ефективність політики безпеки.

3) порівняльно-історичний метод: цей метод використовується для вивчення розвитку правових явищ та процесів у часі. Він дозволяє виявити еволюцію правових систем, політик безпеки або інших явищ та визначити, які чинники вплинули на їхнє становище.

4) ареальний (просторовий) метод: цей метод фокусується на розширенні правових явищ на певній території чи в конкретному регіоні. Він може використовуватися для дослідження поширення певних правових стандартів, норм або політик у різних частинах світу.

5) типологічний метод: Цей метод спрямований на встановлення загального у споріднених правових явищах або системах. Він допомагає класифікувати правові явища за спільними ознаками та розробляти типології для кращого розуміння їх структури та функціонування.

Кожен з цих методів може бути корисним для конкретного дослідження у сфері запобігання злочинності у сфері інформаційних технологій, і вибір методу зазвичай залежить від цілей та завдань дослідження. Комбінування різних методів також може призвести до більш об'єктивного та глибшого розуміння досліджуваних явищ.

Не можна оминути увагою також аксіологічний підхід у методології дослідження запобігання злочинності у сфері інформаційних технологій, що будується на основі принципів аксіології і полягає в таких положеннях: наявність єдиної гуманістичної системи цінностей (безпека, при цьому в тій або іншій інтерпретації, з урахуванням культурного, релігійного, етнічного аспекту буде існувати у вигляді абсолютної цінності); визнання необхідності вивчення і використання історичних та сучасних вчень (безпека як явище динамічне та сама система її забезпечення є цінністю та об'єктом дослідження із часів античності. Певні складові частини безпеки розвивалися багато століть та були об'єктом дослідження філософів, юристів, соціологів та представників інших галузей наукових знань упродовж всього існування системи цінностей).

Даний підхід дає можливість дослідити безпеку як боротьбу протилежностей – безпеки та небезпеки, як двох категорій, що співвідносяться як цінність та антицінність, де цінністю буде виступати відсутність або обмеження до прийнятного рівня загроз та небезпек.

Отже, для пізнання запобігання злочинності у сфері інформаційних технологій було визначено ефективність не одного, а сукупності методологічних підходів, що обґрунтовується складністю самих явищ безпеки та запобіжної діяльності, що складають такі підходи, як діяльнісний, функціональний, системний, порівняльно-правовий та аксіологічний.

Діяльнісний підхід полягає в дослідженні динаміки явища з урахуванням його змінюваності, гнучкості та процедурності. Системний підхід виходить із самої складності явища, що є сукупністю безлічі елементів: державного управління, суб'єктів, процедур, норм тощо. Функціональний підхід надає можливість враховувати напрями впливу під час проведення державної політики у сфері безпеки. Порівняльно-правовий підхід бере за основу порівняння вже досліджені явища для виявлення розбіжностей та схожостей даних явищ. Аксіологічний підхід будується на визначенні безпеки як позитивного, цінного явища для суспільства та держави [308, с. 230–234].

Для здійснення дослідження відповідно до визначеної мети, з огляду на виокремлені завдання та сформовану структуру, також обрано такі методи наукового пізнання:

– діалектичний – для визначення сутності запобігання злочинності у сфері іфнормаційних технологій та його основних складових, важливих для сприйняття наукою кримінального права;

– компаративного аналізу – для зіставлення концепцій представників різних наукових шкіл щодо запобігання злочинності у сфері інформаційних технологій, специфіки формування кримінальної політики з цього питання, сутності трансформації раніше відомих кримінальних правопорушень і виникнення нових суспільно небезпечних посягань, з'ясування сучасного рівня ефективності кримінальної політикив Україні в цілому та на окремих її рівнях;

– герменевтичний, який уможливлює встановлення меж інтерпретацій основних понять інформаційного суспільства, його ознак і складових, необхідних для сприйняття наукою кримінального права, для формування і поглиблення понятійного апарату

запобігання злочинності у сфері інформаційних технологій в Україні;

– аналізу – у висвітленні стану наукової проблеми та виокремлення основних тенденцій трансформації раніше відомих злочинів і виникнення нових суспільно небезпечних діянь під впливом розвитку дистанційних комунікацій;

– синтезу – для розробки доктринальних і концептуальних положень кримінально-правового забезпечення інформаційного суспільства в Україні та пропозицій до удосконалень КК України;

– ретроспективний та метод історизму, а також порівняльно-правовий (як спеціальний метод пізнання) – для дослідження динаміки розвитку суспільних відносин і потреби їх кримінально-правового забезпечення в умовах розвитку суспільно небезпечних посягань в інформаційному суспільстві, аналізу та порівняння наукових і нормативних підходів щодо кримінально-правової охорони суспільних відносин у інформаційному суспільстві, ретроспективного огляду та визначення напрямів актуалізації раніше відомих кримінальних правопорушень і виникнення нових суспільно небезпечних діянь під впливом розвитку запобігання злочинності у сфері інформаційних технологій;

– формально-логічний – задля виявлення вакууму кримінально-правової охорони суспільних відносин щодо запобігання злочинності у сфері інформаційних технологій;

– системний аналіз і метод моделювання соціальних об’єктів як високоорганізованих систем, що разом із методом екстраполяції та імплікації дадуть змогу досягти мети дослідження у визначенні моделі кримінально-правового забезпечення інформаційного суспільства в Україні та формулювання концепції такої політики в Україні [282].

Безумовно, правильно і вкрай своєчасно В. А. Туляков констатує: «у дійсності, поведінка, що відхиляється, стала нормою для значної частини населення в усьому світі», «кількість злих вчинків іде по зростаючій, перебуваючи у прямій залежності від стану аномії у суспільстві, нормосвідомості громадян. І вслід за цим ми накопичуємо досвід їх покарань» [314, с. 67].

Отже, розробка та запровадження нових тактико-стратегічних підходів до кримінально-правового забезпечення інформаційного суспільства є надзвичайно важливою у сучасних умовах, оскільки інформаційні технології стали неодмінною складовою суспільства та

економіки. Для ефективного боротьби з суспільно небезпечними діяннями у сфері інформаційних технологій потрібно враховувати специфіку цих явищ і застосовувати сучасні та інноваційні підходи.

Висновки до Розділу 1

1. Повномасштабне вторгнення російської федерації в Україну та її активні дії у сфері інформаційної війни дійсно висувають інформаційну безпеку на перший план у питаннях національної та міжнародної безпеки. російська федерація використовує інформаційну війну як частину своєї гібридної стратегії для досягнення своїх цілей в Україні та впливу на інші демократичні країни. Для захисту своєї інформаційної інфраструктури та забезпечення свободи слова на тимчасово окупованих територіях, Україна повинна прикладати зусилля щодо підтримки журналістів та медіа організацій, які працюють в цих умовах.

Варто зазначити, що в Україні вже є певні напрацювання з цього приводу. Створення ефективної системи координації та взаємодії між органами державної влади України у сфері стратегічних комунікацій є включає: 1) створення центрального координаційного органу, 2) розробку стратегії інформаційної безпеки; 3) створення механізмів обміну інформацією, 4) підвищення інформаційної грамотності тощо.

2. Терміни, пов’язані з префіксом «кібер-», є предметом наукової дискусії і поки що не мають чіткого та універсального визначення на міжнародному та національному рівнях. Поняття кіберзлочинності, кіберзлочинів, злочинності у сфері інформаційних технологій можуть охоплювати різні види діяльності, пов’язані з використанням інформаційних ресурсів та мереж, і вони можуть включати в себе різні аспекти.

Національні та міжнародні нормативні акти та угоди, що стосуються кіберзлочинності, можуть включати визначення деяких конкретних кримінальних правопорушень, таких як несанкціонований доступ до комп’ютерних систем, крадіжка даних, атаки на інформаційну інфраструктуру тощо. Проте вони можуть бути недостатніми для врахування швидкого розвитку злочинності у сфері інформаційних технологій та нових її форм.

3. На сьогодні виділяють такі етапи розвитку кіберзлочинності: 1 етап – поява кіберзлочинності та субкультури хакерів; 2 етап –

розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності та національних груп хакерів; 3 етап – набуття кіберзлочинністю транснаціонального характеру, поява кібертероризму та міжнародних угруповань хакерів в усіх сферах кіберзлочинності; 4 етап – використання мережі Інтернет в політичних цілях, виникнення таких явищ, як Інтернет-страйк та Інтернет-війна, цілеспрямоване використання кібератак проти урядів окремих держав.

4. Квінтесенцією правового і кримінально-правового розуміння інформаційного суспільства повинна стати специфічна, притаманна інформаційному суспільстві структура суспільних відносин і смисл предметів та цінностей, які зумовлюють утворення таких відносин, виводять на новий рівень суспільні відносини нової доби розвитку людства. Установлення таких особливостей інформаційного суспільства може вважатися об’єктивним лише у процесі міжгалузевого дослідження цього феномена, концепцій його розвитку та прогнозів динаміки суспільних відносин у ньому, а також уразливих від суспільно небезпечних посягань основних складових такого суспільства.

Злочинність у сфері інформаційних технологій і її запобігання у її поєднанні динамізму та статичності, мінливість, структурованість, багатоплановість зумовлюють і відповідну структуру методології її дослідження, що складається з таких складових частин: домінуючого світогляду, типу наукового мислення, філософських засад, наукових парадигм, методологічних підходів та наукових методів.

РОЗДІЛ 2
КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.1. Кількісні та якісні показники злочинності у сфері інформаційних технологій

В останні два десятиліття в Україні спостерігалися кардинальні зміни у політичній, соціальній та економічній сферах. Ці зміни вплинули на всі аспекти суспільного життя, включаючи рівень злочинності, її кількісні показники та характер. Процесуально розширилися та ускладнилися способи вчинення кримінальних правопорушень. Наприклад, злочинці почали активно використовувати нові технічні засоби та інструменти для вчинення кримінальних правопорушень. Мобільність та технічна оснащеність злочинців також значно зросли. Ця тенденція стосується і кримінальних правопорушень у сфері інформаційних технологій, оскільки залученість до комп'ютерних технологій у кримінально протиправній діяльності зросла. Кримінальні правопорушення, пов'язані з комп'ютерними технологіями, характеризуються високим рівнем таємниці, яка обумовлена технічним та соціальним контекстом [102, с. 23].

На цей час можна виділити основні напрямки еволюції злочинності у сфері інформаційних технологій в Україні:

– значний приріст кількісних показників;

– вагомий фінансовий стимул для більшості вчинених комп'ютерних кримінальних правопорушень;

– посилення методів та нові форми вчинення кримінальних правопорушень у сфері інформаційних технологій;

– підвищений професіоналізм осіб, що вчиняють кримінальні правопорушення у сфері інформаційних технологій;

– «помолодшання» комп'ютерних злочинців та збільшення кількості осіб, які раніше не притягали до кримінальної відповідальності;

– значні матеріальні збитки від кримінальних правопорушень у сфері інформаційних технологій у загальному обсязі збитків від інших видів кримінально протиправних діянь;

– зміна акценту в способах вчинення кримінальних правопорушень на використання комп'ютерних мереж;

– перехід злочинності у сфері інформаційних технологій до категорії транснаціональної;

– високий рівень латентності кримінальних правопорушень у сфері інформаційних технологій. Оскільки Інтернет є універсальним та нерегульованим загалом, він не підпадає під конкретну правову юрисдикцію.

Це ускладнюється тим, що дані можуть зберігатися на вебсайтах у різних країнах чи навіть на різних континентах, де законодавство не передбачає відповідальність за зберігання та розповсюдження забороненого контенту. Цю проблему слід вирішувати на міжнародному рівні, можливо, в рамках організацій, таких як ООН та ЮНЕСКО [280, с. 35–36].

Злочинніть у сфері інформаційних технологій – це особливий вид злочинності, пов'язаних із незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки [307, с. 31]. Кримінальний кодекс України вперше визначив окремий розділ щодо цих протирпавних діянь – розділ XVI «Кримінальні правопорушення у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж». Положення цього розділу були змінені та доповнені багато разів, що свідчить про нагальність цієї проблеми у суспільстві.

Слід відзначити, що інформаційні технології стрімко розвиваються та інтегруються в наше суспільство. Наприклад, можливість зберігання та доступу до документів у смартфоні через додаток «Дія» є невід'ємною ознакою розвитку країни. Однак це відкриває нові можливості для кіберзлочинців. Згідно офіційної статистики Офісу Генерального прокурора України, протягом останніх 8 років кількість виявлених кіберзлочинів зросла майже в 7,5 разів [240].

Вчені, такі як Н. М. Ахтирська, О. А. Баранов, Т. В. Варфоломієва, Б. В. Романюк, П. Д. Біленчук та інші вже звернулися до цієї теми, присвячуючи свої дослідження запобіганню злочинності у сфері інформаційних технологій. Це надає значний базис для подальших досліджень, але з кожним днем з'являються нові форми кримінально протиправної діяльності, які також потребують уваги.

Найчастіше використовуючи комп'ютери та Інтернет, вчиняють такі типові правопорушення: порушення авторських прав та суміжних прав (ст. 176), шахрайство (ст. 190), незаконні дії з документами для переказу, платіжними картками та іншими засобами

доступу до банківських рахунків, а також обладнанням для їх створення (ст. 200), ухилення від сплати податків, зборів (обов'язкових платежів) (ст. 212), ввезення, виробництво, збут та поширення порнографічних предметів (ст. 301), незаконне збирання з метою використання або фактичне використання відомостей, які є комерційною або банківською таємницею (ст. 231) [78, с.71].

Однією з найбільш актуальних проблем є кібершахрайство. Наприклад, восени 2021 року часто намагались підробити застосунок «Дія» з метою отримання фальшивих сертифікатів вакцинації, посвідчень водія або навіть паспортів громадянина України. Ці кримінальні правопорушення, хоча були виявлені, мали негативний вплив, оскільки піддавали сумнівам дійсність та безпеку цифрових документів. Ще однією нагальною проблемою в інформаційних технологях є ухилення від оподаткування шляхом оформлення осіб як фізичних осіб-підприємців 3-ї групи. Цей вид працевлаштування в ІТ-сфері можна вважати «напівлегальним», оскільки дозволяє значно знизити суму оподаткування. Іншими словами, при трудових відносинах роботодавець повинен сплачувати 18 % податку на доходи фізичних осіб. Проте з підвищенням рівня злочинності у сфері інформаційних технологій держава створює нові органи та організації, спрямовані на протидію злочинності в ІТ-сфері. При кібератаках важливо звертатися до офіційних органів забезпечення кібербезпеки України, таких як CERT-UA та кіберполіція [335].

Отже, ми зазначили найбільш поширені типи кримінальних правопорушень у сфері інформаційних технологій та навели актуальні приклади. Важливо відзначити, що поки держава не може гарантувати повну безпеку в кіберпросторі, проте кожен рік створюються нові органи або проєкти для виявлення кримінальних правопорушень у цій сфері. Були визначені основні характеристики кіберзлочинів, включаючи важкість визначення місцезнаходження злочинця під час вчинення кримінального правопорушення, слабкі зв'язки між елементами системи доказів, неможливість візуального спостереження та фіксації доказів та широке використання засобів шифрування інформації. Все це значно ускладнює їх виявлення та запобігання. Таким чином, злочинність у сфері інформаційних технологій є невід'ємною частиною сучасного життя, і важливо бути обізнаним з законодавством, щоб уникнути стати співучасником або жертвою інформаційного обману.

Злочинність у сфері інформаційних технологій є складовою злочинності та піддається загальним змінам та закономірностям. У вузькому розумінні поняття кіберзлочинності визначено в Законі України «Про основні засади забезпечення кібербезпеки України». Згідно з цим законом, кіберзлочин визнається «суспільно небезпечною винною діяльністю у кіберпросторі та/або з використанням його, за яку передбачена відповідальність згідно з законодавством України про кримінальну відповідальність, або яка визнана злочином міжнародними договорами України, а кіберзлочинність охоплює сукупність кіберзлочинів» [250].

До основних характеристик кіберзлочинності можна віднести такі: по-перше, кіберзлочини є анонімними та неперсоніфікованими; по-друге, вони вчиняються у кіберпросторі; по-третє, кіберзлочини можуть бути вчинені з великої відстані, розділяючи жертву та кіберзлочинця тисячі кілометрів; по-четверте, кіберзлочинність характеризується високим рівнем латентності; по-п’яте, потрібні відповідні знання та навички в цій сфері [329, с. 402].

Детермінанти кіберзлочинності включають різноманітні суспільні протиріччя у політико-правовій, організаційно-управлінській та культурно-психологічній сферах. Політико-правові аспекти, які визначають злочинність у сфері інформаційних технологій, охоплюють розбіжності між урядами різних країн щодо політики та прав людини в кіберпросторі, а також недостатню політичну волю для належного правового регулювання сфери інформаційної безпеки, що сприяє зростанню кіберзагроз як в межах країни, так і за її межами, включаючи кримінальну протиправну діяльність.

Організаційно-управлінські фактори, які сприяють злочинності у сфері інформаційних технологій, включають недоліки соціального контролю, проявляючись у недооцінці користувачами різних рівнів вимог до інформаційної безпеки, фінансових та наукових проблемах, дефектах в системі організації та недостатньому технічному захисті комп’ютерних мереж, як найбільш вразливого елементу у сучасному технологічному суспільстві. Також до цих факторів належать низький рівень підготовки правоохоронних органів у сфері запобігання злочинності у сфері інформаційних технологій та нестача кваліфікованих кадрів і ефективного науково-методичного супроводу практики виявлення, розкриття та розслідування кіберзлочинів тощо.

Психокультурні чинники злочинності у сфері інформаційних технологій пов'язані із активністю громадян у віртуальному просторі, де окремі особи можуть мати певний «вакуум» у цінностях та світогляді, почуття відчуження від суспільних відносин та недооцінення їхньої важливості.

Аналіз особи кіберзлочинця також є важливим елементом кримінологічного дослідження. Дослідження особи кіберзлочинця дозволяє визначити низку характеристик, за якими можна скласти портрет кіберзлочинця. Цей портрет може бути корисним для ефективного протидії кіберзлочинності.

За статистичними даними Офісу Генерального прокурора, за період 2020–2022 років можна зазначити, що більшість кіберзлочинців є працездатними особами, які не зайняті у роботі та не навчаються (57 %). За сімейним станом вони переважно є одинокими (76 %) або одруженими, але не проживають з родиною (19 %). За статтю, кіберзлочинці переважно чоловіки (91 %), у віці 18–28 років (85 %), громадяни України (95,5 %), які мають базову або професійну середню освіту (77 %). За видом занять, найпоширеніші серед кіберзлочинців є працездатні особи без роботи (57 %), службовці (19 %), робітники (15 %), приватні підприємці (11,4 %). Особи, які навчаються, складають 8,4 %. Працівники господарських товариств становлять 5 % засуджених за вчинення кіберзлочинів [124].

Серед морально-психологічних характеристик кіберзлочинців переважають такі: порушення емоційно-вольової сфери, авантюризм, правовий нігілізм, викривлена система життєвих цінностей, цинізм та корисливість.

Під час аналізу кіберзлочинності в Україні важливо врахувати, що, як і будь-яке інше негативне соціальне явище, її можна оцінити з використанням певних критеріїв, що відображають якісні та кількісні характеристики. Це можна зробити, проаналізувавши злочинність у сфері інформаційних технологій за такими показниками, як рівень, динаміка, коефіцієнт, структура та інші.

На основі аналізу статистичної звітності Офісу Генерального прокурора видно, що рівень злочинності у сфері інформаційних технологій протягом 2020–2022 років є значно високим. Конкретно, протягом цього періоду спостерігається зростання кількості зареєстрованих кіберзлочинів з 2498 до 3415, що на 36,7 % більше

порівняно з показником 2020 року. Це свідчить про суттєве збільшення кількості зареєстрованих кіберзлочинів на 32,5 % порівняно з 2020 роком та на 3,2 % порівняно з 2021 роком [124]. Виходячи з цього, ми робимо висновок, що простежується негативна тенденція, а саме зростання кількості кримінальних правопорушень у цій сфері.

Рівень та динаміка кіберзлочинності за період 2020–2022 рр.

Роки	2020	2021	2022
Всього зареєстровано кіберзлочинів	2498	3310	3415
Динаміка кіберзлочинів у % до попереднього року	–	+32,5 %	+3,2 %

На нашу думку, аналіз рівня кіберзлочинності протягом 2020–2022 років не дає повної картини стосовно цього явища, оскільки злочинність у сфері інформаційних технологій характеризується значним рівнем таємничості. Деякі ознаки цієї таємничості включають негативну реакцію потенційних жертв кіберзлочинів або свідків, недоліки у роботі правоохоронних органів у відповідь на повідомлення про кіберзлочини, та високий технологічний рівень здійснення кіберзлочинів, який охоплює різні сфери життя. Ці фактори таємничості підкреслюють серйозну загрозу злочинності у сфері інформаційних технологій для суспільства, оскільки надають нові можливості кримінальному світові у віртуальному просторі.

Для більш точного вивчення поточного стану кіберзлочинності можна проаналізувати зміну коефіцієнтів кримінальних правопорушень у сфері інформаційних технологій на кожних 100 тисяч населення загалом [124].

Після аналізу наданих даних стає очевидним, що рівень кіберзлочинності був найнижчим у 2020 році (5,9), а найвищим у 2022 році, коли він склав 8,3. З цих результатів очевидно, що коефіцієнт кіберзлочинності у 2022 році збільшився на 5 % порівняно з 2021 роком. Крім того, спостерігається значний зріст коефіцієнта кіберзлочинності з початку досліджуваного періоду до 2022 року.

При аналізі структури кіберзлочинності за період 2020–2022 років, виявлено, що найчастіше відбувалися кримінальні правопорушення, передбачені статтею 361 та статтею 362 Кримінального кодексу України [124].

Структура кіберзлочинності за період 2020–2022 рр.

Роки	2020	2021	2022
Ст. 361 КК України: «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» (%)	47,5 %	50,7 %	41 %
Ст. 361-1 КК України: «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» (%)	4,5 %	1 %	8,2 %
Ст. 361-2 КК України: «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» (%)	5,2 %	4,3 %	1,7 %
Ст. 362 КК України: «Несанкціоновані дії з інформацією, яка обробляється 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» (%)	42 %	43,5 %	48,8 %
Ст. 363 КК України: «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» (%)	0,6 %	0,4 %	0,1 %
Ст. 363-1 КК України: «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» (%)	0,2 %	0,1 %	0,2 %

Варто зазначити, що частка цих конкретних категорій кримінальних порушень була найвищою протягом весь час аналізу, але їх відносна важливість постійно змінювалася. Наприклад, у 2020 році частка статті 361 КК України склала 47,5 %, а статті 362 КК України – 42 %. Проте в наступних роках ці показники постійно збільшувалися, і лише у останньому році аналізуваного періоду кримінальні порушення за статтею 361 КК України зменшилися до 41 %, тоді як порушення за статтею 362 КК України продовжили зростати й

становили у 2022 році 48,8 %. Крім того, з урахуванням отриманих даних можна зазначити, що значущо скоротилась частка порушень, що передбачені статтею 361-2 КК України. Наприклад, їх відносний відсоток зменшився з 5,2 % у 2020 році до 1,7 % у 2022 році. Також важливо відзначити, що в структурі злочинності у сфері інформаційних технологій найменшою є кількість кримінальних порушень, передбачених статтею 363-1 КК України. Частка цього виду порушень залишалась на одному й тому ж рівні як у 2020 році, так і в 2022 році – 0,2 %.

Отже, аналізуючи зміни в структурі кіберзлочинності протягом 2020–2022 років, виявляється дві основні тенденції: негативна та позитивна. Негативна тенденція виявляється у зростанні кількості кримінальних порушень, передбачених статтями 361-1 та 362 КК України, в той час як позитивна тенденція проявляється у зменшенні кількості зареєстрованих кримінальних правопорушень, передбачених статтями 361 та 361-2 КК України.

Аналізуючи частку злочинності у сфері інформаційних технологій у загальній структурі злочинності, слід зазначити, що вона залишається невеликою. Проте це анітрохи не означає, що цей вид злочинності не є суспільно небезпечним. Зокрема, у 2020 році питома вага кіберзлочинності у загальній структурі злочинності становила 0,7 %, у 2021 році вона зросла до 1 %, а у 2022 році ще більше збільшилася до 1,2 %. Загалом можна відзначити негативну тенденцію, оскільки кіберзлочинність набуває обертів і, отже, стає все більш суспільно небезпечним явищем.

Підбиваючи підсумок викладеного, важливо відзначити, що комплексний аналіз кримінологічних характеристик злочинності у сфері інформаційних технологій є надзвичайно актуальним, оскільки це дослідження є основою для подальшого розроблення стратегій запобігання цьому явищу. Детермінаційний комплекс обумовлений важливістю кіберпростору як середовища формування особистості кіберзлочинця. Специфіка криміногенних чинників кіберзлочинності свідчить про відставання можливостей правоохоронних органів від сучасного рівня програмного забезпечення та технологічного прогресу. Опис особистості кіберзлочинця показав, що в більшості випадків це працездатні особи, які не працюють та не навчаються, неодружені, віком від 18 до 28 років. Сучасна кримінологічна ситуація свідчить про швидке зростання злочинності

у сфері інформаційних технологій (+36,7 %). Крім того, спостерігається негативна тенденція – як збільшення кількості кримінально протиправних дій у структурі злочинності, передбачених статтями 361-1 та 362 КК України, так і збільшення питомої ваги цього виду злочинності у загальній структурі всієї злочинності [263].

Враховуючи вище зазначене, стає очевидним, що розвиток кібербезпеки має надзвичайну важливість для України у контексті розроблення стратегій протидії злочинності у сфері інформаційних технологій. Співпраця між усіма державними установами та громадськими організаціями у цій сфері, а також проведення належного кримінологічного аналізу сприятиме ефективному подоланню латентності та зменшенню рівня кримінально протиправних дій у цій сфері.

Слід зазначити, що запобігання кримінальним правопорушенням у сфері інформаційних технологій – це складна та багатогранна задача, спрямована на виявлення та усунення чинників, які сприяли вчиненню кримінально протирпавних діянь. Запобігання включає в себе впровадження системи заходів, спрямованих на виявлення та усунення факторів, що сприяють кримінальним та іншим порушенням. Це дає підстави вважати, що запобігання злочинності включає в себе виявлення факторів, які сприяли вчиненню кримінального правопорушення в межах конкретної дії. Висновки та пропозиції, отримані під час аналізу діяльності, спрямованої на запобігання злочинності у сфері інформаційних технологій, формують основу для дослідження обставин, які сприяють вчиненню кримінальноого правопорушення або його запобіганню в майбутньому у галузі інформатизації суспільства. Це дає підстави для висновків, що запобігання кримінальним правопорушенням у сфері інформаційних технологій полягає в своєчасному виявленні та усуненні факторів, що сприяють їх вчиненню, з дотриманням принципів всебічності, повноти та достовірності. Лише цим способом буде забезпечено повне та якісне запобігання злочинності у сфері інформаційних технологій.

Загалом на сьогодні запобігання злочинності у сфері інформаційних технологій передбачає розуміння негативного впливу, який він має під час вчинення на комп’ютерну інформацію. Цей вплив може бути різних видів, таких як руйнування (втрата) інформації, модифікація (зміна інформації на невірну, правильну за формою та змістом), а також несанкціоноване розголошення її

третім особам. Слід відзначити й ті обставини, які сприяють виникненню саме причини вчинення кримінальних правопорушень у сфері інформаційних технологій.

Підтримуючи позицію науковців, можна розподілити фактори, які сприяли вчиненню кримінальних правопорушень у сфері інформаційних технологій на три групи. До першої групи віднесено умови, в яких використовується комп'ютерна техніка потерпілого. До другої групи виділено умови, пов'язані з сучасним розвитком інноваційних технологій та рівнем технічних знань особи, яка вчинила кримінальне правопорушення у сфері комп'ютерних технологій. До третьої групи належать інші обставини, що стосуються особи комп'ютерного правопорушника. У сфері запобігання кримінальним правопорушенням у галузі комп'ютерних технологій переважати повинен соціальний аспект. Превентивні дії, спрямовані на особу, яка може вчинити кримінальне правопорушення у сфері інформаційних технологій, є ефективнішими, ніж заходи з удосконалення систем захисту інформації. У першому випадку результатом профілактичного впливу є відмова особи від вчинення кримінального правопорушення, оскільки її морально-правова свідомість підвищується. У другому випадку результатом, як правило, є спроба вчинити незакічене кримінальне правопорушення (спроба або замах на на його вчинення), що завжди шкодить суспільним відносинам.

До перешкод на шляху запобігання кримінальним правопорушенням у галузі комп'ютерних технологій можна віднести: 1) нестачу належних засобів у системі органів досудового розслідування; 2) недосконаліть знань, навичок та експертизи посадових осіб органів досудового розслідування в питаннях застосування вказаних засобів; 3) відсутність необхідних тактичних рекомендацій щодо їх використання. Запобігання злочинності у сфері інформаційних технологій, залучаючи новітні інформаційні технології, є можливим при умові наявності належно автоматизованого робочого місця працівників досудового розслідування, обладнаного комп'ютерною технікою, веб-камерою, системними програмами тощо. Використання цих засобів обґрунтоване мінімальними затратами часу, фізичних та інтелектуальних зусиль, а також фінансовими ресурсами [102, с. 24–25].

На основі вивчення практичного досвіду відповідних правоохоронних органів стає очевидним, що, стикаючись з опором

технічних заходів захисту у відношенні незаконного доступу до комп'ютерних систем, злочинці намагаються здобути нові знання та інформацію для подолання цієї перешкоди – нові методи та способи вчинення кримінального правопорушення. Зупинити їх може лише належне правове покарання через суд або реальна загроза судового переслідування. Важливим є виявлення та аналіз причин, що спонукають до злочинності у сфері інформаційних технологій, а також розробка рекомендацій для їх запобігання, включаючи участь правоохоронних органів. Проведені в Україні дослідження показують, що значна частина фахівців, пов'язаних з комп'ютерними технологіями, не мають не лише необхідних навичок, але й правових знань щодо ефективної документації порушень та взаємодії з правоохоронними органами. Це пояснюється тим, що багато неюридичних закладів вищої освіти обмежують правову підготовку лише однією юридичною дисципліною – «Основи права». Більше того, цей курс часто не охоплює аспекти юридичної сутності та особливості комп'ютерних правопорушень, зокрема кримінальних правопорушень. Це призводить до відсутності широкого загалу компетентних юридичних фахівців, які могли б ефективно та комплексно розглядати проблематику комп'ютерної злочинності та правові засоби їй запобігання. Отже, утворюється замкнуте коло вирішення соціальних проблем у сфері запобігання комп'ютерній злочинності [331].

Отже, для запобігання кримінальних правопорушень у сфері інформаційних технологій слід вживати такі заходи:

– інформаційно-аналітичну роботу;

– створення підрозділів технічного захисту інформації в органах влади, правоохоронних органів, збройних силах, на підприємствах, установах, організаціях усіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

– підготовка кадрів для роботи у сфері технічного захисту інформації.

На нашу думку, для попередження кіберзлочинності доречно до даного переліку заходів додати підвищення кваліфікації кадрів, які працюють у цій сфері, а також міжнародне партнерство та обмін досвідом. Слід ще звернути увагу на удосконалення нормативно-правового забезпечення в даній сфері.

Важливою складовою антиспамової системи виявляються профілактичні заходи, спрямовані на запобігання комп'ютерній

злочинності. Більшість експертів зазначають, що уникнути комп'ютерних кримінальних правопорушень набагато простіше та ефективніше, ніж розслідувати їх. Зазвичай виділяють три основні групи превентивних заходів у боротьбі з комп'ютерними кримінальними правопорушеннями: правові, організаційно-технічні та криміналістичні. Інтереси в інформаційній сфері поділяються на особисті, державні та суспільні. Проблема злочинності у сфері інформаційних технологій торкається як окремих осіб, так і цілої країни.

Виходячи з вищесказаного, можна зробити висновок, що запобігання злочинності у сфері інформаційних технологій є важливою складовою національної політики з охорони національних інтересів. Цей вид злочинності став значущою проблемою для світового співтовариства. Правоохоронні органи намагаються протистояти цьому явищу, законодавці приймають нові закони, а правоохоронні структури формують спеціалізовані підрозділи для боротьби з кіберзлочинністю. Для успішного протистояння злочинності у сфері інформаційних технологій важливо залучати фахівців з галузі інформаційних технологій та активних громадян, яких турбує злочинність у віртуальному просторі.

У рамках національної політики необхідно розробити єдину класифікацію та формальну модель кіберзлочинів. Це сприятиме ефективнішій боротьбі та розслідуванню кримінальних правопорушень цього типу. Організація забезпечення інформаційної безпеки повинна бути комплексною і ґрунтуватися на глибокому аналізі можливих негативних наслідків, не пропускаючи жодних значущих аспектів. Аналіз негативних наслідків передбачає обов'язкову ідентифікацію можливих джерел загроз та чинників, які сприяють їх прояву, щоб визначити актуальні загрози інформаційній безпеці.

Для ефективної боротьби зі злочинністю у сфері інформаційних технологій необхідно здійснювати заходи не лише на національному рівні, а й на міжнародному. Необхідно розробляти, стандартизувати та уніфікувати законодавство і програмне забезпечення, що дозволить визначати місце перебування злочинців, які незаконно використовують комп'ютерні мережі та глобальні телекомунікаційні системи. Це є завданням країн, які підписали Європейську конвенцію з питань кіберзлочинності [280, с. 36–37].

У цьому контексті основні складнощі, які виникають при міжнародному правовому регулюванні запобігання злочинності у

сфері інформаційних технологій, полягають у розбіжностях між національними законами щодо кібербезпеки, відсутності чіткої уніфікованої категоріальної системи, недостатньої координації дій правоохоронних органів під час розслідування кіберзлочинів та обміну інформацією про кіберінциденти між країнами, а також недостатнього рівня співробітництва між державними та приватними суб'єктами у цій галузі. Як підкреслює професор Н. А. Зелінська, «потреба в міжнародних правових стандартах обумовлена необхідністю сприяти встановленню кримінально-правового заборону та гармонізувати національне законодавство. Багато країн мають схожість відносно більшості традиційних видів транснаціональної злочинності в межах їх внутрішньодержавного права, але нові види злочинності вимагають об'єднаних визначень. У справах боротьби з кіберзлочинністю проблема гармонізації кримінально-правових заборон набуває особливого значення» [136, с. 582].

Характерною рисою кіберзлочинності є її масштабний та міжнародний характер, що призводить до невисокої ефективності звичайних методів припинення таких кримінальних правопорушень. Важливо відмітити, що для успішної боротьби з кіберзлочинністю держави повинні співпрацювати між собою. Однак цей вид співпраці до певної міри може порушувати державний суверенітет та повноваження у сфері захисту інформації. Найбільш результативною є міжнародна співпраця у боротьбі з кіберзлочинністю та кібертероризмом у тих областях, де існує висока політична довіра між країнами, наприклад, у рамках Європейського Союзу. Запобігання кіберзлочинності є основною метою діяльності Міжнародного центру протидії кіберзлочинності [205].

Створений у 2013 році в Гаазі центр має однією з ключових мет завдань розробку нових методів розслідування кіберзлочинів. У цьому процесі основну роль відіграє Організація Об'єднаних Націй та її спеціалізовані агентства. Специфічні завдання у сфері запобігання високотехнологічним злочинам покладені на Управління ООН з наркотиків та злочинності (United Nations Office on Drugs and Crime – UNODC), в межах якого функціонує Глобальна програма з кіберзлочинності (Global Program on Cybercrime – GPC), а також працює Міжурядова експертна група відкритого складу з кіберзлочинності (Open-ended Intergovernmental Expert Group on Cybercrime). UNODC сприяє довгостроковому і стійкому зростанню

потенціалу для протидії кіберзлочинності, підтримуючи розвиток національних структур та дій.

Превентивні заходи проти кіберзлочинності становлять одну з найбільш актуальних та складних кримінологічних проблем. Зростання кількості кіберзлочинів та постійна модернізація інформаційних технологій, що відкривають нові можливості для вчинення кримінальних правопорушень, актуалізують напрацювання ефективних методів запобігання кримінально протиправним діянням у віртуальному просторі надзвичайно важливим. Ці дії мають потенціал загрожувати глобальним мережам і суспільству в цілому.

Аналізуючи проблему сучасного стану злочинності у сфері інформаційних технологій в Україні, можна зробити такі висновки:

– злочинністьу сфері інформаційних технологій представляє собою один із видів злочинності, який існує порівняно з насильницькою, корисливою, корупційною, екологічною та іншими формами злочинності.

– це тісно пов’язано з іншими формами злочинності, оскільки кримінальні правопорушення у сфері інформаційних технологій часто використовуються як спосіб удосконалення інших кримінальних порушень, таких як крадіжки, шахрайство та інші.

– характеризується високотехнологічним способом виконання, оскільки використовуються ІТ-технології, інформаційно-телекомунікаційні мережі, комп’ютерні пристрої та інші засоби для вчинення кримінальних правопорушень.

– має високий рівень латентності, оскільки виявлення кримінальних правопорушень у віртуальному середовищі ускладнене та неочевидне для більшості населення.

– відзначається високоорганізованим характером та тісно пов’язане з організованою злочинністю, оскільки значна кількість кіберзлочинів вчиняється злочинними групами.

– має «професійний» характер, оскільки особи, що вчиняють кіберзлочини, спеціалізуються в цій сфері та мають необхідні знання та навички для вчинення кримінального правопорушення.

– це транскордонне та транснаціональне явище, оскільки кіберпростір існує поза національними кордонами та дозволяє злочинцям вчиняти злочини в різних країнах та співпрацювати міжнародно [171, с. 356];

– перебуває у стані постійного розвитку, що випливає з неперервного вдосконалення існуючих технологій та створення

нових ІТ-технологій, приваблення нових учасників у сферу інформаційних відносин, розширення кіберпростору за рахунок зростання кількості користувачів мережі Інтернет та використання мобільних комп'ютерних пристроїв, а також переходу все більшої кількості організацій, підприємств та установ до електронного документообігу.

– набула ознак економічної злочинності через те, що більшість кіберзлочинів відбуваються у банківському, фінансовому та корпоративному секторах (інтернет-банкінг, банківський фішинг, кібервимагання тощо), а дії злочинців спрямовані на вилучення доходів та прибутку.

– перетворюється в злочинність політичного спрямування, оскільки представники хакерського руху, спецслужб та силових структур інших країн, а також міжнародних екстремістських і терористичних організацій все активніше займаються незаконною діяльністю в кіберпросторі (DDoS-атаки на урядові веб-ресурси, кібершпигунство щодо інформаційних ресурсів органів державної влади та правоохоронних органів, вчинення кібертерористичних актів тощо).

Вивчення поточного стану та складового комплексу злочинності у сфері інформаційних технологій дозволяє зробити висновок, що запобігання цьому явищу повинна базуватися на таких підходах:

1) міжнародний підхід передбачає об'єднання зусиль правоохоронних органів різних країн та створення спеціальних органів і підрозділів, які займатимуться боротьбою зі злочинністю у сфері інформаційних технологій. Характеристики цього виду злочинності однозначно вказують на те, що ефективне її запобігання неможливе в рамках окремих національних держав без активізації міжнародного співробітництва.

2) правовий підхід пов'язаний із вдосконаленням правових механізмів як на національному, так і на міжнародному рівнях. Цей підхід передбачає введення відповідальності за кіберзлочини. Оскільки жодна держава не здатна ефективно захистити себе від кіберпосягань, приймаючи правові заходи лише на національному рівні, вважається необхідним організувати та реалізувати комплексну програму запобігання злочинності у сфері інформаційних технологій. Ця програма має включати гармонізацію кримінального законодавства щодо кіберзлочинів, розробку та впровадження на міжнародному рівні процесуальних стандартів, які дозволять

ефективно розслідувати кримінальні правопорушення у глобальних інформаційних мережах, міжнародне співробітництво правоохоронних органів у розслідуванні кіберзлочинів на оперативному рівні, а також ефективний механізм вирішення юрисдикційних питань у кіберпросторі.

Отже, міжнародна співпраця виявляється ключовою у ліквідації правового прогалину, яка існує між розвитком інформаційних технологій та реакцією законодавця на них.

3) технічний підхід передбачає запобігання кіберзлочинам через впровадження технічних заходів, спрямованих на забезпечення безпеки в інформаційній сфері, а також створення матеріально-технічної бази підрозділів, що борються з кіберзлочинністю, керуючись принципом «найсучасніша техніка».

4) організаційний підхід спрямований на розробку та впровадження вдосконалених організаційних та профілактичних заходів. Перш за все, потрібно відмовитися від трактування проблеми запобігання кіберзлочинності як подолання існуючих тенденцій і перейти до активного розроблення системи інформаційної безпеки заздалегідь. Необхідно об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян.

Запобігання кіберзлочинності має включати в себе віктимологічну профілактику – підвищення рівня цифрової грамотності населення та сприяння в розповсюдженні індивідуальних засобів захисту особистої інформації. Надзвичайно важливими є глибокі віктимологічні кримінологічні дослідження кіберзлочинності, спрямовані на виявлення об'єктивних закономірностей, детермінант кіберзлочинності, характеристики окремих типів особистості кіберзлочинців, а також різні аспекти забезпечення кібербезпеки [202, с. 137–138].

Підсумовуючи викладене вище, можна зробити висновок, що для ефективного запобігання кримінальним правопорушенням у сфері інформаційних технологій потрібно комплексно підійти до вирішення цієї проблеми. По-перше, потрібно удосконалити національне законодавство, що регулює сферу інфомаційних технологій та привести у відповідність до міжнародних стандартів. По-друге, – готувати висококваліфіковані кадри, які володіють спеціальними

знаннями та розуміються в новітніх технологіях. По-третє, забезпечити правоохоронні органи, що розслідують кримінальні правопорушення в цій сфері відповідним технічним обладнанням.

2.2. Поняття злочинності у сфері інформаційних технологій

Запровадження сучасних інформаційних технологій у всі сфери суспільного життя та стрімкий розвиток інформаційно-телекомунікаційних технологій на базі глобальної мережі Інтернет призвели до розповсюдження високотехнологічних злочинів, пов'язаних із використанням високих інформаційних технологій.

Порушення у сфері інформації настільки розмаїті, що науковцями, національними правовими системами та міжнародним правом наразі ще не сформульовано загальної концепції цих порушень. Також відсутня єдність у термінології та система визнаних юридичних термінів, які б повністю відобразили всю різноманітність незаконних дій і наслідків у сфері інформації, інформаційних технологій, комп'ютерів та їхніх систем, локальних і глобальних інформаційно-телекомунікаційних мереж тощо.

З цієї причини сучасні правові концепції потребують подальшого розвитку у напрямку розуміння сутності, основних характеристик, юридичних причин виникнення, наслідків порушень у сфері інформації, а також їхнього місця у загальній системі незаконної поведінки як на галузевому, так і на загальноправовому рівні, включаючи «міжнародні інформаційні злочини».

Це вказує на кримінально протиправну діяльність суб'єктів міжнародної політики, спрямовану на відкрите спотворення інформаційного простору через масштабну інформаційну експансію, систе-ма-тичну дезінформацію, інформаційну ізоляцію окремих регіонів та створення перешкод для міжнародних інституцій з метою формування ілюзорної суспільної думки, яка відповідає державній міжнародній політиці, не віддзеркалює гуманістичні та правові ідеали сучасного суспільства і загрожує світовому порядку.

1. Зв'язок між порушенням прав та інформацією полягає у впливі порушень на конкретний порядок та правові відносини, що в інформаційному контексті включають такі аспекти: утворення та використання інформаційних ресурсів, заснованих на створенні, зборі, обробці, накопиченні, зберіганні, пошуку, поширенні та наданні інформації.

2. Другий аспект включає створення та використання інформаційних технологій та засобів для їхнього забезпечення.

3. Третя сфера охоплює захист інформації та прав суб'єктів у сфері інформаційних відносин.

Отже, основною характеристикою кримінальних правопорушень в інформаційній сфері є їх зв'язок із процесами обігу інформації, використанням інформаційних ресурсів, застосуванням інформаційних технологій та інформаційно-телекомунікаційних систем. Термін «інформаційне», перш за все, вказує на характер порушень, які можна поділити на дві основні категорії: по-перше, це безпосередні втручання в інформаційні права та свободи суб'єктів, і, по-друге, інші види порушень, які здійснюються через інформаційний простір.

Це означає, що порушення можуть мати інформаційний аспект не лише через їх спрямованість на інформацію або інструменти її обробки, передачі і збереження, але також через використання інформаційних технологій, систем і засобів. При цьому деякі «традиційні» види кримінальних правопорушень, які вчиняються з використанням сучасних інформаційних технологій, можуть стати більш небезпечними для суспільства, що вимагає посилення юридичної відповідальності за них. Це відображається в внесенні відповідних змін до кримінального законодавства.

Отже, інформаційне правопорушення у науці визначається як незаконна, суспільно небезпечна та винна дія (або бездіяльність) особи, що має повну дієздатність, і яка порушує вимоги юридичних норм у сфері інформаційної діяльності (у створенні, передачі, використанні, обробці, зберіганні, захисті інформації тощо), або в іншій галузі за використання інформаційних засобів і технологій, і за яке передбачена юридична відповідальність [310, с. 41].

Навіть за умови, що термін «інформаційне правопорушення» наразі має переважно доктринальний характер і не має чіткого законодавчого визначення, його основні риси можна виділити у численних протиправних діях, які вже передбачені законодавством та мають конкретний юридичний вираз. До таких дій відносяться:

• Незаконний збір, зберігання, обробка, знищення, відтворення, поширення інформації.

• Приховування або неповідомлення інформації.

• Несвоєчасне надання інформації.

• Викривлення або надання завідомо недостовірної (необ'єктивної) інформації.

• Поширення інформації соціально шкідливого характеру.

• Неправомірний доступ до інформації.

• Розголошення інформації з обмеженим доступом.

• Здійснення деструктивного впливу на свідомість особи (або групи осіб, суспільства) за допомогою інформації.

• Створення, використання і поширення шкідливого програмного забезпечення.

• Незаконний доступ та використання систем обробки, зберігання і передавання інформації.

• Несанкціоноване втручання та перешкодження роботі інформаційно-телекомунікаційних систем та їх складових [310, с. 42].

Юридична характеристика інформаційних правопорушень базується на включенні інформаційних складових:

1. Інформаційні елементи можуть виступати як об'єкт правопорушення, коли незаконні дії націлені на порушення інформаційних відносин, або як предмет правопорушення, коли порушується інформація та її носії, інформаційні засоби і системи.

2. Інформаційні компоненти також можуть утворювати об'єктивну сторону правопорушення, вказуючи на спосіб та засіб вчинення незаконної дії, особливо тоді, коли це відбувається за допомогою інформаційних технологій та засобів.

Інші аспекти юридичного складу інформаційного правопорушення не обов'язково включають інформаційні елементи, які впливають на їхню кваліфікацію, але можуть мати певні особливості, що обумовлені інформаційною природою. Це є важливим для розуміння інформаційних правопорушень як феномену в сучасному світі [310, с. 43].

Варто зазначити, що кримінальна відповідальність за порушення у сфері інформаційних технологій в Україні існує з 1994 року. На цей момент Особлива частина Кримінального кодексу України містить Розділ XVI, який регулює правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. [177].

Після подій 2014 року в Україні стало досить важливим створення ефективної системи кібернетичної безпеки. Інформаційна війна між Україною та російською федерацією включає не тільки воєнні операції та інформаційно-психологічні впливові акції, але й

кібернетичні атаки. Це вимагає глибшого дослідження кримінальних правопорушень у сфері інформаційних технологій.

Багато вчених, зокрема В. М. Бутусов, А. В. Голубєв, М. С. Дашян, А. В. Юрасов, Д. П. Біленчук, Є. Д. Скулиш та інші внесли вагомий внесок у вивчення цієї проблеми, аналізуючи злочинність у сфері інформаційних технологій.

У зв'язку з сучасною суспільно-політичною ситуацією в Україні поняття кримінальних правопорушень у сфері інформаційних технологій потребує подальших наукових досліджень та вдосконалення. Термін «кіберзлочинність» часто вживається на рівні з поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій» і «високотехнологічна злочинність». З цих термінів «кіберзлочинність» є найбільш широким та охоплює найбільшу кількість видів кримінально протиправних дій у віртуальному середовищі, а його використання регулюється міжнародним законодавством [139, с. 174].

Як ми уже відмічали, у 2017 році було ухвалено Закон України «Про основні засади забезпечення кібербезпеки України», який визначає юридичні та організаційні принципи забезпечення захисту важливих інтересів особи та суспільства, а також національних інтересів України в кіберпросторі. Цей закон встановлює основні цілі, напрямки та принципи державної політики у сфері кібербезпеки, а також повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, а також основні принципи координації їхньої діяльності в забезпеченні кібербезпеки.

У цьому законі наводяться визначення таким термінам:

– Кібератака означає умірені дії, спрямовані у кіберпросторі з використанням електронних засобів зв'язку, включаючи інформаційно-комунікаційні технології, програмне та апаратне забезпечення, інші технічні та технологічні засоби та обладнання, спрямовані на досягнення різних мет цілей, таких як порушення конфіденційності, цілісності та доступності електронних інформаційних ресурсів, а також отримання несанкціонованого доступу до цих ресурсів, порушення безпеки та функціонування комунікаційних та технологічних систем, а також використання комунікаційних систем, їхніх ресурсів та електронних комунікаційних засобів для здійснення кібератак на інші об'єкти кіберзахисту.

– Кібербезпека означає захищеність важливих інтересів особи та суспільства, а також національних інтересів України під час використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

– Кіберзагроза включає явища і чинники, які потенційно можуть становити небезпеку для важливих національних інтересів України в кіберпросторі, негативно впливають на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

– Кіберзахист представляє собою комплекс заходів, включаючи організаційні, юридичні, інженерно-технічні заходи, а також заходи з криптографічного та технічного захисту інформації. Ці заходи спрямовані на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їхніх наслідків і відновлення стійкості і надійності функціонування комунікаційних і технологічних систем.

– Кіберзлочин (комп'ютерний злочин) представляє собою суспільно небезпечні правопорушення у кіберпросторі або з використанням його, за які передбачена відповідальність згідно із законодавством України щодо кримінальної відповідальності або які визнані злочинами міжнародними договорами України.

– Кіберзлочинність включає в себе сукупність кіберзлочинів [329, с. 403].

Для ефективного запобігання кримінальним правопорушенням у сфері інформаційних технологій та відповідності міжнародному законодавству, Україна приєдналася до Конвенції про кіберзлочинність у 2001 році і ратифікувала її Додатковий протокол у 2006 році. Важливо відзначити, що кримінальне законодавство, а також нормативні акти в інших галузях права, визнають та забезпечують захист законних процесів збору, обробки, накопичення, зберігання, пошуку та поширення інформації, включаючи комп'ютерну інформацію [176, с. 348].

Правопорушення у сфері інформаційних технологій включають різні види кримінальних правопорушень, які вчиняються за допомогою комп'ютерів та мережі Інтернет. Об'єктами цих правопорушень є особисті дані, банківські рахунки, паролі та інша конфіденційна інформація, що належить фізичним і юридичним особам, а також сфера бізнесу та державного сектору. Серед поширених кіберзлочинів на сьогодні можна виділити кібершахрайство,

порушення прав інтелектуальної власності, поширення шкідливого програмного забезпечення та інші подібні правопорушення [95].

Так, більшість українських дослідників обмежувались аналізом окремих аспектів боротьби з кіберзлочинністю, особливо в контексті діяльності компетентних правоохоронних органів та міжнародного співробітництва в цій сфері. Це призвело до невисокого рівня наукового розвитку термінології, пов'язаної з боротьбою з кіберзлочинністю. Деякі вчені, такі як Дж. Арас, О. О. Баєв, Дж. Блумбекер, В. Л. Бурячок, В. М. Бутузов, В. Я. Вовк, А. В. Войціховський, В. Д. Гавловський, Р. Є. Джансараєва, М. О. Кравцова, М. Ю. Літвінов, О. В. Манжай, В. В. Марков, А. А. Протасевич, В. Г. Хахановський, В. В. Чернєй та інші досліджували цю проблематику. Однак жоден із них не провів систематичний аналіз поняття, сутності та ознак боротьби з кіберзлочинністю. Це вказує на необхідність комплексного вивчення цих питань в сучасних умовах.

Глобальна мережа Інтернет об'єднала мільярди людей по всьому світу, надавши унікальні можливості для спілкування, обміну та доступу до інформації, а також для підтримки бізнес-відносин та багатьох інших аспектів. Проте Інтернет також став місцем для великої кількості злочинців, які, використовуючи анонімність та безмежність мережі, здійснюють протиправні дії. З урахуванням стрімкої глобалізації злочинності у сфері інформаційних технологій очевидно, що слід негайно боротися з цим явищем. У цьому контексті дуже важливо зайнятися розробкою правових та наукових механізмів для запобігання комп'ютерним кримінальним правопорушенням.

За визначенням Д. П. Біленчука, кіберзлочинність відноситься до злочинності, яка вчиняється в інформаційному просторі, створеному за допомогою комп'ютера. Цей простір включає дані про осіб, об'єкти, події, явища та процеси, представлені у формі математичних, символьних або будь-яких інших відомостей. Крім того, він охоплює рухи, які відбуваються під час цих процесів. Ця діяльність може мати місце в локальних і глобальних комп'ютерних мережах, або включати дані, які зберігаються в пам'яті фізичних або віртуальних пристроїв та інших носіях, спеціально призначених для зберігання, обробки та передачі таких відомостей. [23, с. 32]. Це визначення є найбільш наближеним до української кримінально-правової доктрини, визначеної у Кримінальному кодексі України [177], однак слід відзначити, що ця дефініція не охоплює усіх аспектів

поняття «злочинність». Наприклад, О. М. Литвак, висловлюючись у своїй монографії, вказує, що злочинність є відносно масовим явищем в кожному суспільстві і складається з сукупності конкретних дій, що визначені кримінальним законом і вчинені на певній території протягом певного періоду часу [185, с. 9].

Отже, важливо відзначити, що Д. П. Біленчук не враховував масовість, територіальний охоплюючий характер та хронологічні аспекти кіберзлочинності. Це означає, що загальна кіберзлочинність повинна бути масовою та охоплювати певний часовий проміжок на території України, щоб вважатися частиною загального явища кіберзлочинності. Навіть якщо питання територіальності у кіберзлочинності може бути складним, оскільки вони відбуваються у віртуальному просторі, якщо об'єкт атаки або сам злочинець виявляються в Україні, такі дії можна розглядати як внутрішню кіберзлочинність.

О. Ю. Іванченко розглядає концепцію кіберзлочинності в подібному значенні, описуючи її як сукупність протиправних дій, які відбуваються у віртуальному просторі за допомогою комп'ютерних систем та мереж, використовуючи різні засоби віртуального простору, і спрямовані проти комп'ютерних систем, мереж та комп'ютерних даних [139, с. 173].

Загальною рисою, а також обмеженням у розумінні кіберзлочинності, що визначається авторами, є їхня увага, спрямована виключно на специфіку кіберзлочинів та кіберпростору з відмовою враховувати загальну сутність злочинності взагалі.

Щодо класифікації кіберзлочинів:

1)порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем включає наступні види:

– незаконний доступ, який може бути досягнутий через шлях взлому, обману та інші способи;

– нелегальне перехоплення комп'ютерних даних;

– втручання в дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

– Ввтручання в систему, включаючи намірене створення серйозних перешкод для функціонування комп'ютерної системи, наприклад, через розподілені атаки на ключову інформаційну інфраструктуру;

– зловживання пристроями, яке охоплює створення, продаж, придбання для використання, поширення пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою вчинення кіберзлочинів.

– вчинення правопорушень, пов'язаних з комп'ютерами, включаючи фальсифікацію і шахрайство, за допомогою комп'ютерних засобів;

– вчинення правопорушень, пов'язаних із змістом інформації, таких як дитяча порнографія, расизм і ксенофобія;

– вчинення правопорушень, які стосуються порушення авторських та суміжних прав, таких як незаконне відтворення та використання комп'ютерних програм, аудіо/відео матеріалів і інших видів цифрової продукції, а також баз даних і книг.

Враховуючи мотивацію злочинців, можна умовно класифікувати кримінальні правопорушення у сфері інформаційних технологій на такі категорії: кібершахрайство з метою фінансового збагачення; кібершахрайство з метою незаконного отримання або обороту інформацією (для особистого користування або подальшого продажу); втручання у роботу інформаційних систем з метою незаконного доступу до автоматизованих систем управління (з метою завдання шкоди для отримання винагороди або ушкодження конкурентів); та інші види кримінальних правопорушень [270].

Кіберзлочинність означає порушення закону, яке відбувається у віртуальному просторі, відомому як кіберпростір. Цей простір можна описати як інформаційне середовище, що формується за допомогою комп'ютерів, де знаходяться дані про осіб, об'єкти, факти та події у різних форматах. Ці дані перебувають у русі завдяки локальним і глобальним комп'ютерним системам. Відомості також можуть бути збережені в пам'яті фізичних чи віртуальних пристроїв, що призначені спеціально для їх зберігання, обробки та передачі [16, с. 86].

На нашу думку, під кіберзлочинністю варто розуміти умисне, незаконне використання будь-якого комунікаційного пристрою для вчинення або сприяння вчиненню будь-яких протиправних дій у сфері інформаційних технологій.

На основі цього можемо сформувати ознаки кіберзлочинності:

1. Ці протиправні дії відбуваються у віртуальному просторі або в межах комп'ютерних мереж. Віртуальний простір є моделюваним за допомогою комп'ютера інформаційним простором, де розміщуються дані про осіб, факти, явища та процеси, представлені у

математичному, символьному або іншому форматі. Ці відомості перебувають у русі завдяки локальним і глобальним комп'ютерним мережам і зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, призначеного спеціально для зберігання, обробки та передачі даних.

2. Кіберзлочини вчиняються з використанням комп'ютерних систем або через комп'ютерні мережі та інші доступні засоби до віртуального простору, а також спрямовані проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Електронно-обчислювальна техніка може бути інструментом для здійснення кримінального правопорушення або об'єктом самого кримінального правопорушення. Наразі найбільш поширеною є класифікація кіберзлочинів на агресивні та неагресивні. До першої групи відносяться такі види: кібертероризм, загрози фізичного насильства (наприклад, передані через електронну пошту), кіберпереслідування, кіберсталкінг (незаконні сексуальні домагання та переслідування через Інтернет), дитяча порнографія (створення та поширення порнографічних матеріалів із зображенням дітей, доступ до них) [349, с. 112]. До другої категорії належать такі види кіберзлочинів: кіберкрадіжка, кібервандалізм, кібершахрайство, кібершпигунство, поширення спаму та вірусних програм.

Вчені аналізують поняття кіберзлочину з двох аспектів:

1. У вузькому розумінні (комп'ютерний злочин) – це будь-яке незаконне діяння, вчинене за допомогою електронних операцій, яке спрямоване на порушення безпеки комп'ютерних систем і оброблюваних ними даних.

2. У широкому розумінні (пов'язане з комп'ютерами) – це будь-яке протиправне діяння, пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння, пропозицію або поширення інформації за допомогою комп'ютерних систем або мереж [295, с.146].

Ми вважаємо, що на сучасному етапі розвитку суспільства та безпосередньо інформаційних технологій, кіберзлочинність варто розглядати у широкому розумінні, тому що майже кожне четверте правопорушення вчиняється за допомогою технічних пристроїв, а не лише коп'ютерів.

Проте кіберзлочинність охоплює не лише вчинки, що здійснюються у глобальній мережі Інтернет. Вона розповсюджується на всі

види кримінальних правопорушень, що відбуваються в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси та техніка можуть бути об'єктом або метою злочинних посягань, а також середовищем, в якому відбуваються правопорушення, та засобом або інструментом кримінальних діянь. [16, с. 87].

К. В. Тарасюк визначає «кіберзлочини» як суспільно небезпечні дії, які у будь-який спосіб пов'язані з кіберпростором та комп'ютерною інформацією, що обробляється комп'ютерами. Такі дії мають свої особливості, такі як висока прихованість, складність виявлення та розслідування, труднощі у доведенні їх в суді, переважно транснаціональний характер, особливо з використанням мережі Інтернет, і призводять до великих збитків навіть від одного кримінального правопорушення. [306, с. 178].

Н. В. Савчук розглядає «кіберзлочинність» як термін, що включає в себе комп'ютерну злочинність (де комп'ютер є об'єктом кримінального правопорушення, а інформаційна безпека є предметом кримінального правопорушення), а також інші дії, де комп'ютер виступає як знаряддя або засіб для вчинення правопорушень щодо власності, авторських прав, громадської безпеки, моралі та інших аспектів [284 с. 339].

О. Є. Користін та інші концептуалізують кіберзлочинність як сукупність правопорушень, які відбуваються у кіберпросторі, використовуючи комп'ютерні системи та комп'ютерні мережі, або здійснюються шляхом доступу до кіберпростору через різні засоби, і спрямовані на комп'ютерні системи, комп'ютерні мережі та дані [171, с. 46].

До комп'ютерної ж злочинності, на погляд одних учених, відносяться всі протизаконні дії, за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом [143, с.14], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури і методи, а також процес комп'ютерного опрацювання даних [3, с. 72].

В. Лісовий визначає цю ознаку інакше: «електронна обробка інформації» – незалежно від того, на якій стадії кримінального правопорушення вона застосовувалася [191, с. 87].

Більшість дослідників вважають «кіберзлочинність» та «комп'ютерні злочини» синонімами. Проте В. А. Намоконов та Т. Л. Тропіна підкреслюють їх відмінність, вказуючи, що перше термін є більш широким і точно відображає сутність злочинності в інформаційному

просторі. Також слід зазначити, що Рада Європи у листопаді 2001 року, приймаючи Конвенцію про кіберзлочинність, використала саме термін «cybercrime», а не «computer crime» [5, с. 34].

Проте в національній юридичній літературі перевага віддається поняттю «комп'ютерна злочинність». За В. Бутузовим, «комп'ютерні злочини» та «кіберзлочини» представляють собою різні категорії кримінальних порушень у сфері високих інформаційних технологій, які класифікуються за такими ознаками:

– ознакою віднесення певних кримінальних порушень до «комп'ютерних злочинів» є використання комп'ютерної техніки як знаряддя для здійснення кримінального порушення. Автор вказує, що об'єктом порушення є суспільні відносини у сфері автоматизованої обробки інформації;

– ознакою віднесення кримінальних порушень до «кіберзлочинів» є специфічне середовище, у якому вони вчиняються – кіберпростір (середовище комп'ютерних систем та мереж) [74, с. 119].

А. Музика та Д. Азаров визначають тотожність понять «кіберзлочини» та «злочини у сфері комп'ютерної інформації» та наголошують, що «кіберзлочини» треба визначати як «злочини у сфері комп'ютерної інформації» [4, с. 5], проте з цим не можна погодитися, оскільки предметом деяких кримінальних правопорушень, передбачених Розділом XVI КК України, є не тільки комп'ютерна інформація, а й об'єкти авторського права, комп'ютерні програми, носії інформації, платіжні картки тощо.

На нашу думку, поняття «кіберзлочини» та «комп'ютерні злочини» – це різні поняття. «Кіберзлочинність» більш ширше поняття, а «комп'ютерні злочини» – вужче поняття, яке передбачає використання лише компютерної техніки під час вчинення даних кримінальних правопорушень або коли комп'ютерна техніка, або інформація, яка міститься на ній, є предметом даного кримінального правопорушення. А якщо говорити про «кіберзлочини», то тут уже потрібно розглядати ширше коло застосовуваних злочинцями технічних пристроїв, які працюють по типу комп'ютерів, але таким не є.

М. В. Карчевський запропонував включити в національне законодавство термін «кримінальні правопорушення у сфері використання інформаційних технологій». Він розумів це як «один із типів порушень у сфері інформаційної безпеки, що передбачені Кримінальним кодексом України, які є суспільно небезпечними та

вчинені суб'єктом кримінального правопорушення, використовуючи обчислювальну техніку і завдаючи шкоду відносинам у сфері задоволення інформаційних потреб». При аналізі чинного Кримінального кодексу можна зробити висновок, що до цих порушень слід віднести посягання, описані в статтях 361, 361-1, 361-2, 362, 363, 363-1, 376-1 КК. [145, с. 11].

М. М. Дмитрук має відмінну позицію від М. В. Карчевського. Він вказує на приклад порушення авторських та суміжних прав, яке полягає в втручанні в роботу ЕОМ і завдає шкоду «відносинам у сфері реалізації інформаційних потреб», використовуючи саме «засоби обчислювальної техніки». Проте М. В. Карчевський не розглядає цей склад кримінального правопорушення в цьому аспекті у своїй роботі. Інші аргументи вказаного вченого підтримують позицію щодо класифікації кримінальних правопорушень, передбачених у Розділі XVI Особливої частини Кримінального кодексу України, як «злочини у сфері використання ІТ». [118, с. 16].

Цікава позиція, в якій поняття «комп'ютерний злочин» замінюється на «інформаційний злочин», причому ЕОМ – один із видів засобів для вчинення кримінального правопорушення, а об'єктом є не сам комп'ютер, а дані, які обробляються за допомогою комп'ютера [16, с. 80–81].

Отже, вченими запропоновано визначати кіберзлочинність як сукупність визначених кримінальним законом дій, що вчинені на певній території або стосовно об'єктів, розташованих на цій території протягом певного періоду часу, у віртуальному просторі шляхом негативного впливу на комп'ютерні системи, комп'ютерні мережі і комп'ютерні дані [75].

На сучасному етапі термін «боротьба із кіберзлочинністю» є досить незвичним для вітчизняної науки, хоча кримінально протиправні дії, які використовують всесвітню мережу Інтернет, несуть великий рівень суспільної небезпеки. Цей термін уже не перший рік є в науковому обігу, проте автори переважно не розглядають його сутність та ознаки, а зосереджуються на значенні та алгоритмах реалізації. Тому одним із способів вирішення проблеми боротьби зі злочинністю у сфері інформаційних технологій вбачається розробка теоретичних основ цього деструктивного суспільного явища.

Терміни «кіберзлочинність» та «комп'ютерна злочинність» часто вживаються поряд, проте не є повністю синонімами. Дійсно, ці

терміни дуже близькі, але мають відмінності. Поняття «кіберзлочинність» (в англомовному варіанті – cybercrime) є ширшим, ніж «комп'ютерна злочинність» (computer crime), і точніше відображає природу цього явища, як злочинність в інформаційному просторі.

Так, Оксфордський тлумачний словник пояснює префікс «cyber» як складову частину складних слів. Його значення пов'язане з інформаційними технологіями, мережею Інтернет та віртуальною реальністю. Подібне визначення надає і Кембриджський словник. Отже, «cybercrime» – це злочинність, яка стосується як використання комп'ютерів, так і використання інформаційних технологій та глобальних мереж. З іншого боку, термін «computer crime» в основному описує злочини проти комп'ютерів або комп'ютерних даних [295, с. 48.].

Згідно з думкою Н. В. Савчук, кіберзлочинність включає комп'ютерні та інші посягання, де комп'ютер є інструментом або засобом здійснення злочину проти власності, авторських прав, громадської безпеки, моралі та інших аспектів. Отже, поняття «кіберзлочинність» є більш широким, ніж «комп'ютерна злочинність».

Важливо відзначити, що у законодавстві України, зокрема у Законі «Про основи національної безпеки України» та «Доктрині інформаційної безпеки України» згадується про «комп'ютерну злочинність» та «комп'ютерний тероризм», але вони не мають чіткого визначення. У Законі «Про боротьбу з тероризмом» термін «комп'ютерний тероризм» не згадується, а його аналогію вживають як «технологічний тероризм».

У 1986 році у Парижі група експертів Організації економічного співробітництва та розвитку визначила комп'ютерний злочин як «будь-яку незаконну, неетичну або заборонену поведінку, спрямовану на автоматизовану обробку та передачу даних». З урахуванням необхідності скоординованої міжнародної взаємодії, такі міжнародні організації, як Інтерпол, Організація економічного співробітництва і розвитку, Група Восьми (G8), Рада Європи, ООН здійснюють протидію кіберзлочинності, що в значній мірі сприяє визначенню кола кримінальних правопорушень у сфері інформаційних відносин. 13 вересня 1989 року Рада Європи прийняла Рекомендацію № R89 (9) Комітету міністрів Ради Європи щодо кримінальних правопорушень, пов'язаних з комп'ютером, де було

зроблено першу спробу визначити поняття та коло протиправних діянь, пов'язаних із використанням комп'ютерів.

В Рекомендаціях № R (95)13 щодо проблем кримінального процесуального права, пов'язаних з інформаційними технологіями, Рада Європи замінила вираз «злочин з використанням комп'ютера» на «злочин, пов'язаний з використанням комп'ютерних технологій». У цьому документі особливий акцент робиться на тому, що кримінальні правопорушення, що стосуються використання інформаційних технологій, можуть бути вчинені не тільки за допомогою окремого комп'ютера, але й комп'ютерної системи, яка може бути як об'єктом, так і середовищем для вчинення кримінального правопорушення [253, с. 96–97].

За період з 1985 по 1989 роки Спеціальний Комітет експертів з питань злочинності, пов'язаної з комп'ютерами, відповідав за розроблення Рекомендації № 89, яку Комітет Міністрів Ради Європи схвалив 13 вересня 1989 року. Цей документ включав перелік правопорушень і рекомендацій країнам-учасницям ЄС щодо формування єдиної стратегії у сфері кримінальної боротьби з комп'ютерними кримінальними правопорушеннями. Рекомендація також підкреслювала необхідність досягнення міжнародного консенсусу з питань криміналізації деяких кримінальних правопорушень, пов'язаних з комп'ютерами.

У жовтні 1999 року під час саміту Європейської Ради у місті Тампере (Фінляндія) Європейська комісія представила Рамкове рішення під назвою «eEurope». Цей проєкт мав на меті використання потенціалу нових технологій та підвищення безпеки комп'ютерних мереж.

У Рамковому рішенні містилися пропозиції Європейської комісії щодо створення європейського простору безпеки, свободи і правопорядку. Крім того, цей документ надав визначення понять, таких як «інформаційна система», «комп'ютерні дані», «юридична особа» і «несанкціонований доступ до бази даних». Відповідно до цього рамкового рішення кримінально карались такі дії:

– незаконний доступ до інформаційної системи;

– незаконне вторгнення в систему (умисне перешкодження або порушення функціонування інформаційної системи шляхом введення, передачі, пошкодження, знищення, псування, зміни, придушення або відтворення секретних комп'ютерних даних);

– незаконне проникнення в базу даних [8, с. 5].

Як ми визначали вище, твердження М. В. Карчевського про віднесення певних дій до «кримінальних правопорушень в сфері використання ІТ» лишається без обґрунтування. Якщо прийняти цю позицію, то виходить, що порушення авторських та суміжних прав через втручання в роботу ЕОМ не завдає шкоди «відносинам у сфері реалізації інформаційної потреби» і не вчиняється з використанням саме «засобів обчислювальної техніки». Проте реальність є абсолютно протилежною. Інші аргументи від М. В. Карчевського, які підтримують класифікацію кримінальних правопорушень, передбачених у Розділі XVI Особливої частини КК України, як «кримінальні правопорушення в сфері використання ІТ», не наведено.

Щоб розібратися, що означає «інформаційні технології» та чи можна систему злочинів, передбачених у Розділі XVI особливої частини КК України, визначити як «кримінальні правопорушення у сфері інформаційних технологій», розглянемо етимологію поняття «інформаційні технології».

«Інформаційна технологія», згідно статті 1 Закону України «Про Національну програму інформатизації», представляє собою спеціально організовану систему інформаційних процесів, яка використовує засоби обчислювальної техніки для ефективної обробки даних з високою швидкістю, швидким пошуком інформації, розподілом даних та наданням доступу до джерел інформації незалежно від їхнього місцезнаходження [248]. Таке ж визначення цього поняття міститься у «Методиці визначення належності бюджетних програм до сфери інформатизації» затвердженої Наказом Держкомзв'язку від 06.06.2003 № 97 [201]. Наведене визначення є достатньо широким і не дозволяє з'ясувати точну відповідність між термінами «сфера інформаційних технологій» та «сукупність суспільних відносин, що охороняються положеннями Розділу XVI особливої частини КК України».

У березні 2000 року на спеціальному саміті Ради Європи «Європа на шляху інновацій та знань», який відбувся в Лісабоні, було визначено та уточнено поняття «комп'ютерні злочини». Це поняття інтерпретується у широкому контексті як будь-який злочин, пов'язаний з використанням інформаційних технологій. Також було зауважено, що терміни «комп'ютерні злочини», «злочини у сфері високих технологій» та «кіберзлочинність» є взаємозамінними і включають в себе: а) використання інформаційно-комунікаційних

мереж без географічних обмежень; б) передачу віртуальних та змінних даних.

До основних порушень у цій галузі законодавство Євросоюзу та національне законодавство країн-членів відносять такі дії:

– кримінальні правопорушення, які впливають на особисте життя: незаконний збір, зберігання, зміна, розкриття або розповсюдження особистої інформації;

– правопорушення, пов'язані з контентом: поширення порнографії, зокрема дитячої, расистських висловлювань та інформації, що спонукає до насильства;

– економічні правопорушення, несанкціонований доступ та саботаж: незаконне використання систем (наприклад, хакерство, комп'ютерні атаки, поширення вірусів, комп'ютерна шпигунівка, фальсифікація даних, комп'ютерне шахрайство);

– порушення у сфері інтелектуальної власності: порушення правового захисту комп'ютерних програм і баз даних, авторських і суміжних прав [8, с. 5].

В Конвенції про кіберзлочинність від 23.11.2001 р. (ратиф. Закону України № 2824-IV від 07.09.2005 р.) до кіберзлочинів віднесено:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6));

2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8));

3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією (ст. 9);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10).

У Преамбулі Конвенції про кіберзлочинність також зазначено, що її положення спрямовані на «боротьбу із кіберзлочинністю» та «захист законних інтересів у ході використання та розвитку інформаційних технологій». Отже, відповідно до змісту системи кримінальних правопорушень, передбаченої Конвенцією про кіберзлочинність, відповідає визначенню «кіберзлочин», яке міститься в положеннях пункту 8) статті 1 Закону України «Про основні засади

забезпечення кібербезпеки України», а захист «інформаційних технологій» є одним з завдань Конвенції про кіберзлочинність.

У зв'язку з цим, важливим є питання про те, яким чином визначається система кримінальних правопорушень у кримінальному законодавстві інших країн, до яких Кримінальний кодекс України є подібним за своєю структурою.

В Кримінальному кодексі Грузії Глава XXXV визначає цю систему злочинів як «Кіберзлочини», таку ж назву має Глава 30 у Кримінальному кодексі Азербайджану.

У Кримінальному кодексі Вірменії вказана група порушень, відповідно до Глави 24, має назву «Злочини проти безпеки комп'ютерної інформації». Аналогічно, у Кримінальному кодексі Киргизької Республіки, за Главою 42, ця група порушень визначається як «Злочини проти інформаційної безпеки», і цей розділ має однакову назву з Розділом XII Кримінального кодексу Республіки Таджикистан.

У Кримінальному кодексі Туркменістану ця група порушень, відповідно до Розділу XIII, отримує назву «Злочини в сфері комп'ютерної інформації» і включає одну Главу 33 з підзаголовком «Злочини в сфері інформатики і зв'язку». У Кримінальному кодексі Естонії, згідно з Главою 14, ця група порушень визначається як «Злочини в сфері комп'ютерної інформації та обробки даних». Глава 7 Кримінального кодексу Казахстану має назву «Кримінальні правопорушення в сфері інформатизації та зв'язку». У Кримінальному кодексі Литовської Республіки відповідна група порушень, згідно з Главою XXX, іменується як «Злочини проти інформатики». І лише у Кримінальному кодексі Республіки Узбекистан, відповідно до Глави XX-1, ця група порушень визначається як «Злочини в сфері інформаційних технологій».

Отже, дослідження назви системи порушень більшості держав ближнього зарубіжжя свідчить, що вказана система кримінально протиправних діянь визначається, як:

1) кіберзлочини;

2) злочини проти інформаційної безпеки;

3) злочини проти комп'ютерної інформації (або інформатики) та зв'язку;

4) злочини в сфері інформаційних технологій.

Виходячи з вищесказаного, більшість країн ближнього зарубіжжя не включають конкретні предмети або засоби у назву кримінальних правопорушень у сфері інформаційних технологій. Такий метод

визначення системи кримінального правопорушення, коли конкретні аспекти суспільних відносин перераховуються в назві, застосовується у Розділах XX, XIV, XIII, але цей підхід важко вважати успішним.

Ураховуючи, що поняття кіберзлочину або комп'ютерного кримінального правопорушення, згідно з чинним Законом України «Про основні засади забезпечення кібербезпеки України», застосовується до порушень, які порушують суспільні відносини, охороняються положеннями Розділу XVI Особливої частини Кримінального кодексу України, а також до порушень, які порушують будь-які інші суспільні відносини за допомогою інформаційних технологій, було доцільно визначити дії, за які передбачена відповідальність згідно зі статтями 361, 361-1, 361-2, 362, 363, 363-1 Кримінального кодексу України, як «кримінальні правопорушення у сфері інформаційних технологій», подібно до Кримінального кодексу Узбекистану. При цьому розподілення на кіберзлочини та кримінальні правопорушення у сфері ІТ є досить умовним, оскільки законодавче поняття «інформаційні технології» охоплює більш широкий спектр суспільних відносин, ніж ті, що охороняються положеннями Розділу XVI Особливої частини Кримінального кодексу України. Крім того, терміни «кіберзлочин» та «інформаційні технології» використовуються у Конвенції про кіберзлочинність як різні поняття [118].

Дослідження наукових праць вказує на те, що вчені використовують різні терміни, такі як «кіберзлочини», «злочини у сфері інформаційних технологій», «комп'ютерні злочини» та інші. Однак з їх визначень очевидно, що ці поняття мають схожий зміст.

Наприклад, В. О. Голубєв описує кіберзлочини як незаконну діяльність, спрямовану на порушення суспільних відносин і особистої чи корпоративної безпеки, коли особи обмінюються електронними даними [96]. М. С. Дашян зазначає, що комп'ютерні злочини – це порушення чужих прав та інтересів по відношенню до автоматизованих систем обробки даних [113, с. 288].

С. А. Правдюк визначає під комп'ютерними кримінальними правопорушеннями протиправні та суспільно небезпечні дії, які вчиняються деліктоздатним суб'єктом з використанням комп'ютера чи інших комп'ютерних систем (мереж). Ці дії порушують нормальний режим охорони, обробки і передачі даних в комп'ютерах (комп'ютерних системах) [232, с. 220–221].

А. В. Юрасов вказує, що поняття «кіберзлочини» охоплює комп'ютерну злочинність (де комп'ютер – предмет кримінального правопорушення, а інформаційна безпека – його об'єкт) та інші посягання, де комп'ютер є знаряддям або способом вчинення кримінального правопорушення проти власності, майнових та немайнових прав, громадської безпеки тощо [340, с. 480]. П. Д. Біленчук під кіберзлочинами розуміє кримінальні правопорушення у сфері використання комп'ютерних та інформаційних мереж, наслідком яких є протиправне заволодіння даними [23, с. 32–34].

Слід відзначити, що саме це визначення найбільш точно відображає офіційну кримінально-правову позицію в Україні, яка закріплена у Кримінальному кодексі. Так, як правильно вказує Є. Д. Скулиш, кіберзлочинність як явище виникло під впливом еволюції комп'ютерних та інформаційних технологій. Основною метою злочинців є отримання персональних та корпоративних даних, які самі по собі є цінністю. За допомогою цих даних злочинці можуть незаконно заволодіти фінансами, нематеріальними активами, майновими або немайновими правами та іншими цінностями [296, с. 94].

Саме тому пропонуємо авторське визначення кримінальних правопорушень у сфері інформаційних технологій, під якими варто розуміти кримінально протиправні діяння (дія або бездіяльність), які посягають на права та свободи осіб, держави шляхом використання таким чином, порушуючи інформаційну безпеку, задля матеріальної чи особистої вигоди.

Кримінальні правопорушення у сфері інформаційних технологій є ширшим поняттям за комп'ютерні кримінальні правопорушення, а тому варто включити до цього поняття інші правопорушення, для вчинення яких застосовується комп'ютер та використовується Інтернет [49].

2.3. Кримінологічний портрет особи злочинця, що вчиняє кримінальні правопорушення у сфері інформаційних технологій

Швидкий прогрес у технологіях, який спостерігається в останні роки, спричинив прискорення різних процесів як на рівні держави, так і на недержавному рівні. Паралельно з цим злочинці все активніше використовують інформаційні технології в кримінально протирпавних цілях. Це сприяє швидкості вчинення кримінальних

правопорушень та дозволяє злочинцям тривалий час залишатися «невиявленими» для правоохоронних органів.

Крім того, кримінальні правопорушення, пов'язані з інформаційними технологіями, характеризуються підвищеною суспільною небезпекою, оскільки впливають на інші сфери, такі як власність, національна та громадська безпека тощо. Питома вага цих кримінальних порушень у відсотках є значно вищою, ніж 10 років тому. Отже, однією з найактуальніших проблем сучасності є розробка оновленої стратегії запобігання злочинності у сфері інформаційних технологій, оскільки ця сфера дуже швидко змінюється, а злочинці постійно вдосконалюють методи вчинення кримінальних дій, що є невідомими правоохоронним органам.

Аналіз кримінальних правопорушень, які включають використання інформаційних технологій, та розробка ефективних стратегій їх запобігання неможливі без урахування типових особистісних рис тих, хто вчиняє кіберзлочини. Саме тому важливим є вивчення характерних ознак осіб, які є причетні до кримінально протирпавних дій у сфері інформаційних технологій.

У дослідженнях щодо запобігання злочинності в галузі інформаційних технологій та розробці кримінологічної моделі запобігання кіберзлочинам брали участь видатні науковці, такі як Н. Ахтирська, В. Бутузов, С. Буяджи, В. Гавловський, І. Європіна, О. Іванченко, М. Кравцова, Л. Скалозуб, Є. Скулиш та інші. Проте на сьогодні в кримінології відсутні вичерпні дослідження, що охоплюють типовий кримінологічний портрет осіб, які вчиняють кримінальні правопорушення у сфері інформаційних технологій.

Аналіз особистісних рис осіб, які вчиняють кримінальні порушення у сфері інформаційних технологій, не є новим. Зокрема, М. О. Кравцова надає кримінологічну характеристику особистості кіберзлочинця. Згідно з її висновками, кіберзлочинці переважно є працездатними, але безробітними, неодруженими чоловіками, чиї морально-психологічні риси включають корисливість та правовий нігілізм, поєднані зі специфічним комплексом сваволі та ілюзій, що диктується особливостями кіберпростору [173, с. 20]. Незважаючи на те, що на даний момент активно ведуться дослідження у цьому напрямку, оскільки кримінальна активність у сфері інформаційних технологій постійно зростає та еволюціонує.

При аналізі осіб, які вчиняють кримінальні порушення у галузі інформаційних технологій, можна розглядати їхні дії як з точки зору

характеристик протиправних кримінально протирпавних актів, так і з погляду особистісних рис – суб'єктів, що здійснюють ці порушення. Наприклад, фахівці з університету Норідж (приватний військовий університет, розташований у Нортфілді, штат Вермонт, США) виділяють різні типи кіберзлочинців:

– «ідентифікаційні злодії» – це зазвичай кіберзлочинці, які намагаються незаконно отримати доступ до особистих даних потерпілих, таких як ім'я, адреса, телефонний номер, місце роботи, банківський рахунок, дані кредитних карток та номер соціального страхування, і використовують цю інформацію для фінансових маніпуляцій, вигадуючи себе за потерпілого;

– «інтернет-сталкери» – це категорія злочинців, які незаконно контролюють онлайн-діяльність своїх жертв, використовуючи соціальні мережі та шкідливі програми, які здатні невидимо відстежувати комп'ютерну активність особистості;

– «пікери» (або «шахраї», «фішери») – це злочинці, які намагаються отримати особисту або конфіденційну інформацію через комп'ютери жертв, часто шляхом створення фішингових вебсайтів;

– «кібертерористи» – це високорівнева категорія злочинців з політичними мотивами, які намагаються втручатися у комп'ютерні системи та мережі корпорацій, держав або організацій, крадучи дані та завдаючи шкоду країнам, підприємствам, організаціям або окремим особам [402].

Сучасний рівень технологій призвів до спеціалізації хакерів у конкретних напрямах. Ця спеціалізація дозволяє виділити «групи за інтересами» серед загальної кількості хакерів. Наприклад, «крекери» (cracker) – це експерти, що спеціалізуються на обходженні механізмів безпеки; «кранчери» (cruncher) – це фахівці зі зняття захисту програмного забезпечення від копіювання; «крешери» (cruncher) – це ентузіасти, що активно експериментують з комп'ютерною системою для дослідження можливостей управління нею. Залежно від специфічності їхньої діяльності, хакерів можна класифікувати у трійку груп: Software hackers, чи софтверні хакери, займаються тим, що «зламують» програмне забезпечення. Це численна група хакерів, і шкода від діяльності цих людей вимірюється мільйонами доларів.

– Phreks – особа, яка віддає перевагу альтернативним способам оплати телефонних та інших комунікаційних послуг (наприклад,

вона може змусити сусідів оплатити телефон за неї, використовуючи блокувальний пристрій).

– Кардери представляють собою осіб, які змінюють програмування телефонних карток таким чином, що на картці виникає практично безмежний кредит для телефонних розмов. Ця група може бути найнебезпечнішою серед фрікерів, оскільки вони мають глибокі знання у галузі радіоелектроніки та програмування мікросхем. Кардери представляють потенційну загрозу, і служби безпеки уважно контролюють їхні дії.

– Net hacers – це група осіб, яка відокремилася від фрікерів з активним розвитком технологій у сфері мереж. Мережевий хакер повинен мати глибокі знання про мережі зв'язку та методи їх захисту. Вони вторгаються в захист Інтернет-серверів, атакують державні та корпоративні інформаційні системи. Ці атаки можуть мати різні мети, включаючи промисловий шпіонаж на замовлення конкуруючих компаній. Серед цієї категорії основний фокус припадає на осіб, які взламують програмне забезпечення, включаючи зняття захисту з комерційних версій програмних продуктів та створення реєстраційних ключів для безкоштовних програм тощо.

До найнебезпечнішої групи хакерів слід віднести тих, хто створює комп'ютерні віруси. Їхня діяльність може завдати шкоди будь-якому користувачеві комп'ютерних систем. Розповсюдження вірусів здійснюється різними способами, проте останнім часом найчастіше вони поширюються через електронну пошту [128, с. 121–122].

У свою чергу, Р. Мітчелл визначив типи кіберзлочинців, які відрізняються своїм рівнем майстерності та мотивацією, зокрема це такі:

– початківці;
– кіберпанки;
– внутрішні (внутрішня загроза);
– кодери;
– інформаційні воїни/кібертерористи;
– старі хакери охорони;
– професійні кіберзлочинці [128, с. 121–122].

Деякі науковці виокремлюють такі типи кіберзлочинців:

– порушники правил користування ЕОМ (несанкціоноване використання комп'ютерів, поширення вірусів і т. п.);

– «білокомірцеві» злочинці;

– «комп'ютерні шпигуни» – підготовлені професіонали, метою яких є отримання важливих стратегічних даних про супротивника в економічній, політичній, технічній та інших сферах;

– «хакери» («одержимі програмісти») – технічно підготовлені особи, які, вчиняючи кримінальні правопорушення, часто не переслідують при цьому прямих матеріальних вигод (для них має значення самоствердження, помста за образу, бажання пожартувати тощо).

Інші дослідники виділяють три основні категорії комп'ютерних злочинців:

– Експерти, яких відрізняє поєднання високого професіоналізму у сфері комп'ютерної техніки та програмування з елементами фанатизму та творчості.

– Особи, які страждають від нового виду психічних розладів, відомих як «інформаційні хвороби» або «комп'ютерні фобії».

– Професійні комп'ютерні злочинці, які мають чітко виражену корисливу мету. В науковій спільноті іноді зустрічається уточнення назви для другої категорії порушників. Запропоновано називати їх особами, що страждають від нового типу психічних порушень – інформаційних хвороб або комп'ютерних фобій. При виявленні подібних обставин під час розслідування призначається судово-психіатрична експертиза для встановлення осудності злочинця на момент вчинення ним кримінально протиправних дій [350].

Кримінологічна суть кримінального правопорушення та особистість його виконавця найкраще виявляються у мотивації кримінально протиправної діяльності, оскільки саме у мотивах відображається не окрема риса особистості, а в певному сенсі всесвітність особи та всі її характеристики та особливості.

Мотив передбачає думку й волю, свідомість і дію, виступаючи основною пружиною, що направляє вольовий процес та надає йому певний зміст. Отже, мотив є однією з найсуттєвіших психологічних концепцій, за допомогою якої розкривається внутрішня природа людських вчинків та їх сутність. Це важливий компонент психологічної структури будь-якої людської діяльності, її рушійна сила, що позначає внутрішню (психологічну) причину вчинків конкретної особи. Зазвичай мотив означає внутрішнє підпорядкування, яким керується особа, вчиняючи суспільно небезпечні дії. Це суб'єктивний стимул для людських вчинків, який виражає рушійну силу особистості та пов'язаний із задоволенням її потреб.

В цілому більшість дослідників виокремлюють такі групи мотивів, типових для вчинення кіберзлочинів:

1) корисливий мотив;

2) хуліганські мотиви;

3) помста;

4) політичні мотиви.

На нашу думку, перелік груп мотивів, притаманних для вчинення злочинності у сфері інформаційних технологій, потрібно розширити, додавши емоційний мотив – самореалізацію та мотив гри. Дуже часто кіберзлочинці вчиняють протиправні діяння саме з метою самореалізації та доведення самому собі своєї професійної спроможності, а також задоволення свого его за допомогою гри в можливості.

Взагалі доречно всі групи мотивів вчинення кіберзлочинів укрупнити і виділити три групи:

– раціональні мотиви (сюди можуть входити корисливі, політичні мотиви, релігійні мотиви);

– емоційні мотиви (мотив помсти, мотив гри);

– моральні мотиви (хуліганські мотиви, мотив справедливості);

– змішані мотиви (дуже часто поєднуються емоційні з моральними мотивами).

Вітчизняні дослідники вказують, що, незважаючи на суттєві зміни у технологіях, внутрішній аспект цього типу кримінальних правопорушень залишається практично незмінним. У більшості цих злочинців спостерігається прагнення до особистої вигоди. Злочинці переважно мають корисливі мотиви, особливо у вчиненні дій, пов’язаних з поширенням шкідливих програм [174, с. 90].

Мотивація, яка спонукає кіберзлочинців до вчинення кримінальних правопорушень, має різноманітний характер. Переважно це наркисистичні та матеріальні мотиви, шпигунство, особисті причини, саботаж у політичних, релігійних або інших переконаннях, а також прагнення підвищити свою самооцінку.

Аналіз кримінальних проваджень підтверджує, що основними мотивами кіберзлочинців є матеріальна вигода (86 %), бажання помститися (6 %), потреба у самоствердженні (3 %), хуліганство (2 %), мотивація для кар’єри (1 %), а також інші особисті нематеріальні інтереси (2 %). Таким чином, можна зазначити, що мотиви кіберзлочинів відповідають загальним схемам та не суттєво відрізняються від мотивів інших видів кримінальних правопорушень. У

більшості випадків, інформація про мотив правопорушення знаходиться у вироку суду, оскільки встановлення мотиву ґрунтується на суб'єктивних показниках та зізнаннях винної особи. Детальний аналіз мотивації вчиненого діяння фактично не проводиться ні під час досудового розслідування, ні під час судового розгляду. Це призводить до ситуації, коли багато вчинених кримінальних правопорушень відображаються як мотивовані лише матеріальною вигодою або хуліганськими імпульсами. Вчені часто використовують терміни, такі як «дослідницький інтерес» чи «допитливість», для опису мотивації вчинення кіберзлочинів, що викликає додаткове непорозуміння.

Наприклад, Л. В. Борисова вказує на те, що серед основних мотивів комп'ютерних кримінальних правопорушень важливе місце займає «унікальний за своєю суттю мотив – інтелектуальна боротьба між людиною і комп'ютерною системою» [69, с. 76].

Деякі дослідники вказали на наявність особливого класу комп'ютерних злочинців – «осіб з психічними розладами, які страждають від нового типу психічних захворювань – інформаційних хвороб або комп'ютерних фобій». В. В. Крилов, зважаючи на мотиви кримінального правопорушення, рівень професійної підготовки та соціальний статус, виділяє такі категорії комп'ютерних злочинців:

1. «хакери» – особи, які вважають взлом комп'ютерних систем особистим викликом і проникають у них для отримання повного доступу та задоволення своїх амбіцій;
2. «шпигуни» – особи, які відомі зламуванням комп'ютерів для отримання конфіденційної інформації, яка може бути використана в політичних, військових або економічних цілях;
3. «терористи» – особи, які розглядають взлом інформаційних систем як засіб створення загрози з метою політичного впливу;
4. «корисливі злочинці» – особи, які намагаються проникнути в інформаційні системи з метою особистого фінансового чи іншого матеріального збагачення;
5. «вандали» – особи, які взламовують інформаційні системи з метою їх подальшого руйнування;
6. психічно хворі особи, які страждають від нового типу психічних захворювань – інформаційних хвороб або комп'ютерних фобій [174, с. 91].

Беручи до уваги, що фобія є психічною аномалією, а не хворобою, тому не виключає осудності, і те, що «інформаційна» хвороба залишається лише припущенням, хотілося б зазначити таке. Фахівці, юристи та кримінологи рідко зверталися до неусвідомленого. Описуючи мотиви кримінальних правопорушень загалом або окремих їх видів, дослідники зазвичай працюють тільки з усвідомлюваними мотивами, рідко звертаючись до сфери неусвідомленого для встановлення справжніх мотивів кримінально протиправної поведінки, або взагалі ігноруючи цю сферу через складність та глибину проблеми.

На нашу думку, у всіх наведених випадках доцільно говорити не про якісь особливі мотиви вчинення кіберзлочинів, а саме про мотиви, що належать до сфери неусвідомленого, передусім про мотиви ствердження і самовиявлення, а також про так звані ігрові мотиви. Отже, аналізуючи мотивацію кіберзлочинів, не потрібно шукати якісь специфічні мотиви (чи намагатися їх вигадати), а слід працювати з вже встановленими поняттями та категоріями. Особливість кіберзлочинності полягає не так в мотивах вчинення кримінальних правопорушень цього типу, як в особливостях їх вчинення, обумовлених специфікою середовища та засобів здійснення.

Розглядаючи мотиви кіберзлочинів слід мати на увазі, що, як правильно вказує А. В. Савченко, різноманітні мотиви не тільки не виключають один одного, але й можуть доповнювати та підсилювати один одного [283, с. 25]. Маючи на увазі специфіку кіберзлочинів, можливі різні комбінації та змішування мотивів під час їх вчинення (в залежності від характеристик злочинця, особливостей виникнення та формування). Як відомо, мотив є важливою обставиною, що характеризує ступінь суспільної небезпеки самого злочину та характер та ступінь суспільної небезпеки особи, що його вчинила.

Отже, правильне встановлення мотиву кримінальних правопорушень у сфері інформаційних технологій дозволяє не тільки уникнути помилок під час кваліфікації, але й досягти успішної реалізації принципів справедливості та невідворотності покарання. З практичної точки зору встановлення мотиву та мети вчинення кримінальних правопорушень у сфері інформаційних технологій дозволяє зрозуміти внутрішню суть кримінально протиправної поведінки винного та виявити наявність чи відсутність сукупності кримінальних правопорушень. Наприклад, експерти вказують, що корисливий мотив під

час вчинення «Несанкціонованого доступу до комп'ютерної інформації» може свідчити про те, що це кримінальне правопорушення було вчинене разом із такими порушеннями, як «Порушення авторського права та суміжних прав» (ст. 176 КК України), «Вимагання» (ст. 189 КК України), «Розголошення комерційної таємниці» (ст. 232 КК України) та іншими. Встановлення ж мети – передачі інформації іноземній державі, іноземній організації або її представникам під час вчинення громадянином України кримінального правопорушення «Несанкціонований доступ до комп'ютерної інформації» свідчить про схожість цього протиправного діяння зі злочином, передбаченим ст. 111 КК України «Державна зрада». Також встановлення мети – порушення роботи автоматизованої системи, що забезпечує функціонування атомної електростанції, може вказувати на сукупність вчинення досліджуваного кримінального правопорушення із правопорушенням «Диверсія» (ст. 113 КК України) [174, с. 92].

Отже, встановлення мотивів кримінальних правопорушень у сфері інформаційних технологій відіграє значущу, а в деяких випадках ключову роль для правильної кваліфікації вчиненого діяння (особливо з огляду на корисливу спрямованість кіберзлочинів та поширеність їх вчинення разом із іншими злочинами), а також сприяє виявленню причин (перш за все, суб'єктивних) та умов їх вчинення.

Існує поширене помилкове уявлення про кіберзлочинців, яке передбачає, що вони володіють різними навичками та злочинним досвідом, що дає їм можливість ініціювати різноманітні напади та отримувати значні фінансові вигоди. Однак недавні дослідження серед членів закритої підпільної спільноти показали, що більшість кіберзлочинців заробляють в межах від 1000 до 3000 доларів США на місяць, причому лише 20 % отримують значно більше, а саме 20 000 доларів на місяць і більше [357].

Для надання кримінологічного аналізу злочинців у сфері інформаційних технологій дослідники використали відкритодоступні джерела в мережі Інтернет, зокрема інформацію про розшукувані особи за даними Федерального бюро розслідування США [366]. Перелік злочинців, який включає 42 підозрюваних у кіберзлочинах, доступний на відповідному веб-сайті «Найрозшукуваніші злочинці», які розшукуються ФБР за цими звинуваченнями. Дослідження виявило соціально значущі характеристики міжнародних кіберзлочинців. Зокрема, відповідно до вікового критерію, більшість осіб (60 %), які

перебувають у федеральному та міжнародному розшуку, мають вік від 20 до 35 років. За статевою ознакою більшість підозрюваних у кіберзлочинах є чоловіками [366].

Варто відмітити, що кіберзлочинці, враховуючи досвід США, відносяться до категорії особливо небезпечних злочинців, які завдають велику матеріальну шкоду державі, підприємствам, установам, організаціям, інформаційній безпеці. Крім того, у списку відсутні безпосередньо громадяни США [366].

Отже, здійснення об'єктивних висновків щодо географічних характеристик особистостей кіберзлочинців є досить складним завданням. Однак, базуючись на вказаних даних, можна з певною ймовірністю підтвердити, що більшість злочинців є громадянами країн, де запобігання кіберзлочинам має низький рівень, зокрема, це стосується держав Середнього та Далекого Сходу, таких як Пакистан, Індія, Іран, Сирія, В'єтнам тощо. Крім того, важливими є політичні чинники, зокрема, ставлення урядів конкретних країн до цього негативного явища, що впливає на значну кількість підозрюваних у кіберзлочинах з Північної Кореї та Китаю.

Використовуючи міжнародний досвід, було також проведено аналіз та вивчення статистики стосовно осіб, які вчиняють кримінальні правопорушення у сфері інформаційних технологій в Україні. Дослідження було спрямоване на осіб, яким оголошено про підозру за вчинення кримінальних правопорушень, передбачених ч. 3, 4 ст. 190 КК України [177].

Під час 2020 року службами Департаменту кіберполіції Національної поліції України було виявлено та розкрито шахрайство, яке відбулося за допомогою незаконних операцій з використанням електронно-обчислювальної техніки. У цьому контексті було ініційовано 2012 кримінальних проваджень, у яких 321 особа була оголошена підозра.

Аналіз отриманих даних дозволив виявити статеві тенденції у злочинності в галузі інформаційних технологій. Зокрема, було виявлено, що 72 % кримінальних проваджень були відкриті щодо чоловіків, тоді як 23 % – щодо жінок. Це свідчить про те, що основними виконавцями кіберзлочинів є чоловіки, але відзначається й певний відсоток жінок. Також доцільно врахувати ще один критерій – кримінальні правопорушення, вчинені з участю осіб обох статей (8 %).

Кібершахрайство тісно пов’язане з сектором інформаційних технологій (IT). Згідно з опитуванням DOU щодо заробітної плати, станом на 2020 рік лише 20 % працівниць, які займаються роботою або є фрілансерами в сфері інформаційних технологій, є жінками [127]. Зазначені дані вказують на рівень залученості жінок у технічні сфери, що тотожно навчанню у технічних вищих навчальних закладах або в технічній підтримці того чи іншого державного і приватного підприємства. Однак, згідно з тими самими результатами вищезазначеного опитування, тенденція збільшення з кожним роком кількості осіб жіночої статі у сфері IT становить у середньому 2 %. Так, у 2011 частка жінок із вказаними інтересами становила лише 7 % [184].

Розглядаючи соціально-демографічні показники особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій, варто почати з віку таких осіб. Аналізуючи статистику Офісу Генерального прокурора, потрібно відмітити, що відповідні кримінальні правопорушення вчиняли громадяни віком від 17 до 48 року, тобто від підлітків до осіб старшого віку [249].

Додатково було виявлено, що основну частину складають особи у віці від 20 до 35 років і це узгоджується з проведеним раніше дослідженням щодо осіб, які розшукуються ФБР США за підозрою у вчиненні кіберзлочинів. З аналізу підозрюваних цієї категорії видно, що лише 26 % мали одну чи більше вищих освіт, 21 % – мали середньо-спеціальну освіту. Більшість кібершахраїв мали повну середню освіту. Проте це не означає, що українська шкільна програма надає основи для вчинення шахрайства з використанням комп’ютерних мереж. Враховуючи наведений факт, можна зробити висновок, що особа з категорії кіберзлочинців, зазвичай, самостійно здобуває або вже отримала освіту у сфері високих інформаційних технологій (комп’ютерна безпека, програмування, сучасні тенденції розвитку комп’ютерних мереж) поза будь-яким навчальним закладом, без педагогічної підтримки.

Щодо національної приналежності, важливо відзначити, що більшість кримінальних правопорушень у сфері інформаційних технологій вчиняють українські громадяни, водночас іноземці становлять невеликий відсоток. Також варто зауважити, що у більшості випадків особи, які порушують закон у цій області, це роблять на території свого проживання (71 %).

Базуючись на аналізі слідчих матеріалів швейцарської поліції, можна виявити характеристичні особливості комп'ютерних злочинців. Більшість з них є чоловіками. 87 % злочинців мають вік від 20 до 40 років, тоді як 13 % є старшими 40 років. Більшість злочинців (77 %) мають середній рівень інтелектуального розвитку, 21 % – вище середнього, і лише 2 % – нижче середнього. 52 % порушників мають спеціальну підготовку у сфері автоматизованої обробки інформації. Значна частина порушників (97 %) є співробітниками обчислювальних центрів і відповідних установ, включаючи 30 % злочинців, які безпосередньо займаються експлуатацією комп'ютерних пристроїв. Більшість злочинців здійснюють протиправні дії з метою збагачення. Дослідження справ щодо комп'ютерного шпіонажу показало, що з усіх порушників 93 % – чоловіки. Вік 92 % злочинців коливався між 20 та 40 роками, а решта були старшими за 40 років. Щодо освіти, 50 % порушників закінчили школи, 44 % мали середню освіту, і лише 6 % – вищу. Щодо рівня інтелектуального розвитку, у 93 % злочинців був середній рівень, у інших – вище середнього. Понад 80 % правопорушників мали спеціальну підготовку в галузі автоматизованої обробки інформації. Серед них 48 % виявилися співробітниками установ і фірм, де вчинялися комп'ютерні кримінальні правопорушення. Щодо аналізу слідчих матеріалів щодо комп'ютерного саботажу в Швейцарії, то виявлено, що 25 % злочинців були молодші за 20 років, а інші мали вік від 20 до 40 років. За оцінками експертів, 90 % осіб, які вчинили кримінальні правопорушення, мали середній рівень інтелектуального розвитку, а решта – вище середнього. Усі злочинці мали спеціальну підготовку, і половина з них були співробітниками постраждалих установ, організацій та фірм. [69, с. 77–78].

Аналізуючи вищевказану інформацію пропонуємо виділити такі групи кіберзлочинців залежно від їх професійних навичок:

1. Особи, які не є працівниками IT сфери, але мають певні навички – такі особи рідко вчиняють маштабні кібератаки, вони обмежуються дрібними шахрайськими діями в цій сфері. Такі правопорушення можуть вчинятися без обмеження в часі, а також привязаності до місця роботи чи проживання.

2. Особи, які є найманими працівниками IT сфери – особи, які працюють на посадах менеджерів компютерних мереж, тощо (такі особи найчастіше вчиняють правопорушення даного виду з власних

корисливих мотивів. Такі правопорушення вчиняються протягом робочого часу і в межах місця роботи).

3. Особи, які займають керівні посади в ІТ сфері – такі особи вчиняють кіберзлочини з корисливих мотивів, але уже із корупційною складовою. Ці кримінальні правопорушення найчастіше вчиняються під час робочого часу та в межах місця роботи. Але є певні особливості даної категорії злочинців: вони можуть вчиняти кіберзлочини самостійно, а можуть залучати до їх вчинення підлеглих працівників. Діже часто правопорушення, які вчиняються даною категорією осіб виявляють високу латентність і вчиняються протягом тривалого часу.

4. Контрагенти підприємств ІТ сфери. Великий відсоток кримінальних правопорушень в цій сфері вчиняється із залученням даної категорії осіб. Особливістю цієї категорії осіб є те, що вони дуже рідко вчиняють кіберзлочини, найчастіше вони виступають пособниками.

Науковці наголошують, що вказані соціально-демографічні аспекти, що стосуються кібершахраїв, представляють лише зовнішній аспект. Щоб уявити собі внутрішній світ осіб, які вчинили кримінальне правопорушення, необхідно вивчити їхні особисті характеристики. Серед цих аспектів особистості можна виокремити спрямованість, риси характеру, моральні якості, знання, навички, звички, рівень особистісної культури і інші. Щодо морально-психологічних рис кібершахраїв, вони в загальних рисах подібні до характеристик шахрайства загалом [184, с. 65–68].

Сучасні дослідження вказують на деякі характеристики, які є найвідмітнішими психологічними особливостями шахрайств: мотиви, спрямовані на матеріальну вигоду, жага наживи, жадібність, прагнення накопичувати матеріальні блага та представлення про комфортне життя. Ці особливості супроводжуються вищим рівнем інтелекту, особливо у порівнянні з іншими категоріями злочинців, вмінням швидко адаптуватися до сучасних умов життя, холоднокровністю, вмінням керувати собою, розумінням психології інших осіб та здатністю набудувати їхню довіру. Також важливі аспекти включають прояв співчуття та співпереживання, акторські таланти, спостережливість, невимушеність у поведінці, готовність до використання обману, схильність до паразитизму, моральну розбещеність, лицемірство, нахабність і грубість, вміння впливати на інших психологічними методами та інші аспекти [70, с. 111].

Проте наша думка полягає в тому, що кримінальна активність у сфері інформаційних технологій є найбільш небезпечним видом злочинності для суспільства, де поняття обману і зловживання довірою витримані відмінно. Сучасний злочинець може не обов'язково мати акторські здібності, відчувати необхідність ефектно брехати або взагалі приховувати свою поведінку.

Найбільш важливими психологічними особливостями особистості є мотиви злочинців, які виявляють сильне прагнення до самореалізації на соціальному рівні (це пов'язано з бажанням отримати визнання від найближчого оточення – родини, друзів, знайомих, колег по роботі) і на індивідуальному рівні (це пов'язано з бажанням підвищити власну самооцінку та зміцнити самоповагу через здійснення дій, що сприяють, на думку особистості, подоланню будь-яких психологічних слабкостей). Не менш характерними для кіберзлочинців є ігрові мотиви, які є особливими для осіб, які вчиняють злочини не лише або не стільки з метою матеріальної вигоди, скільки для самої гри та ризику, для отримання гострих відчуттів. Ці мотиви дуже виразно виявляються в ситуаціях, де відбувається інтелектуальна боротьба та змагання в спритності, де потрібна кмітливість, вміння максимально використовувати сприятливі обставини і швидко приймати рішення [184].

На основі вище вказаного можна виділити групи мотивів вчинення кіберзлочинів та відповідно до цих мотивів групи злочинців, залежно від їх професійних навичок:

1. Корисливі мотиви (власне збагачення) найчастіше притаманні злочинцям в «білих комірцях».
2. Корисливі мотиви у вигляді корупції – притаманні державним службовцям, які займають високі посади.
3. Ігнорування норм етики на робочому місці – притаманні професійним порушникам, які працюють в інформаційному середовищі.
4. Інші мотиви антисуспільної спрямованості – професійним злочинцям, хакерам, особам з психічними порушеннями, які працюють в інформаційному середовищі.

Практична складова нашого дослідження спрямована на аналіз основних характеристик особи кіберзлочинця, специфіку конкретного кримінального правопорушення та його віктимологічний аспект. Якщо спростити і класифікувати злочини за основними категоріями (об'єкт, суб'єкт та їх похідні), можна відмітити певні

аналогії між традиційною типологією злочинної поведінки та її сучасними віртуальними проявами. Наприклад, злочини проти національної безпеки та віртуальні аспекти інформаційної війни, кібертероризм; порушення прав на життя та здоров'я через систематичне тискування особи у соціальних мережах, спонукання до самогубства або убивство через втручання в систему автоматизованого управління транспортом; порушення прав на статеву свободу та сексуальне знущання над неповнолітніми під час спілкування в мережі; крадіжки віртуального майна та шахрайство в Інтернеті, фішинг, вішинг, кеш-трепінг тощо [403].

У свою чергу, основний пласт злочинів, звичайно із певними застереженнями, поділяється на політичні, корисливі, агресивні, анархічні та необережні[93,с.440].

Віддавши визнання загальноприйнятій кримінологічній теорії та використовуючи аналогію як метод наукового пізнання, ми пропонуємо класифікувати кіберзлочинців згідно наведених вище видів кримінальних правопорушень на такі категорії:

– ідеологічно мотивовані (імпульсивні). Ці особи зазвичай раніше не були судимі, можуть мати певні специфічні знання та навички або бути аматорами. В основному, їхня діяльність спрямована на виклик системі;

– корисливі, часто мають кримінальні записи за посягання на власність. Основна мотивація – отримання матеріальної вигоди. Вони часто працюють у групах, тщательно планують свої дії та можуть бути наемниками (в залежності від виду посягання, вони можуть бути як простими шахрайами, так і професійними "чорними" хакерами);

– анархічні (вандали). Ці особи мають антигромадянські наміри і використовують комп'ютер як засіб для здійснення антисоціальної злочинної поведінки. Вони суб'єктивно вважають, що суспільство в цілому, окремі особи або організації потребують дезорганізації [221].

Отже, в контексті нашого дослідження пропонується класифікація кримінальних правопорушень у сфері інформаційних технологій на три категорії: ті, в яких технічний пристрій є об'єктом суспільно небезпечної діяльності; ті, де він є проміжним інструментом між кількома етапами досягнення кримінально протиправної мети; та ті, де він виступає лише засобом (платформою) для планування кримінального правопорушення.

Для аналізу структури особи кіберзлочинця за А. Ф. Зелінським, ми розглядаємо загальний психологічний портрет такого правопорушника [137, с. 57]. Для більш ефективного та глибокого аналізу необхідно звузити кількість осіб і зосередитися лише на певних незаконних діяннях, пов'язаних із мережею. Водночас ми відмовляємося від зазначеної нами типологізації за мотивом. Таким чином, нашим пріоритетом є дослідження структури «хакера», оскільки саме цей загальний образ широко відомий у сучасній масовій культурі та особливо відзначений навіть серед тих, хто має віддалене уявлення про сутність інформаційних технологій. Щодо семантики, сам термін англійського походження («hack») дослівно вказує на атаку або злам. Хакер розглядається суспільством як креативна особистість, що володіє специфічними знаннями у галузі програмування та може нестандартним чином обійти системи безпеки на комп'ютері.

Такий індивід є чоловіком, неодруженим, не мав конфліктів з законом раніше й бездітнім. Його вік коливається від 14 до 25 років, з піковою активністю навколо 16 років. Це пояснюється особливостями вікової психології, оскільки саме в юнацтві є період амбіцій, пошуку власного "Я" і прагнення до життєвого успіху, при цьому досвіду та відповідних ресурсів бракує. Соціолог Роберт К. Мертон називає цей розрив між цілями та засобами «аномією». Хакери демонструють високу продуктивність та адаптивність у справах харчування та побутового комфорту. Щодо освіти, вони переважно мають вищу або середню спеціальну освіту (наприклад, технічні спеціалісти). Їхнє місце проживання знаходиться в віддалених районах міста, а житло зазвичай здається в оренду. Важливі цінності є суперечливими, особа не вважає себе порушником та уявляє себе анонімним генієм. Ці люди відзначаються інтровертністю, малим колом довірених осіб і працюють самостійно. Важливо підкреслити, що ми розглядали лише «класичного хакера», що є значно вужчим поняттям, ніж кіберзлочинець, та охоплює тільки усталену у суспільстві (лінгвістичну) форму сприйняття цього явища.

Вивчення явища кіберзлочинності потребує аналізу віктимологічного аспекту, оскільки часто вчинення протиправних дій зумовлене поведінкою потенційної жертви. В сучасний період спостерігається поширення нових видів обману, таких як фішинг (поєднання слів «voice» та «fishing») та смішинг (поєднання «СМС» та «fishing»). Звичайно, жертвами цих правопорушень стають

переважно літні або вразливі особи, які легко піддаються зовнішньому впливу, незалежно від віку. Шахраї обирають потенційних потерпілих з уважністю, використовуючи публічно доступну інформацію, а іноді навіть використовуючи злам конфіденційних даних. Важливо зазначити, що сучасна людина часто сама розміщує особисті дані в мережі, що значно спрощує завдання зловмисникам.

Головною причиною вразливості громадян і високого ризику стати жертвами є уявлення про безпеку, оскільки, як ми вже наголошували, кіберпростір є своєрідним територіальним простором, метавимкненням для усвідомлення. Людина часто навіть не усвідомлює можливих загроз, вступаючи в анонімні відносини, які практично не піддаються нормативному регулюванню. Неосвідомленість про основи безпеки в онлайні, надмірна довірливість і легковажність роблять особу дуже вразливою перед будь-якими шахраями. Як ми вже вказували, потенційні жертви кіберзлочинів можуть бути випадковими або цільовими. Це спостереження має вагу, оскільки на практиці саме випадкові особи можуть потрапити під фармінг (розповсюдження серед широкого кола осіб), тоді як конкретно обрані можуть стати об'єктом кіберпереслідування (здійснюваного з певною метою щодо певної особи). [85, с. 125]. Правильна поведінка після потрапляння у роль жертви грає суттєву роль у запобіганні злочинності в галузі інформаційних технологій. Часто лише після реального атаки особа задумується про необхідність здорового підходу до безпеки в онлайні. У цьому важливо усунути абстрактне сприйняття жертвою кіберзлочину та надати їй розуміння реальних можливостей отримання компенсації за заподіяну шкоду [327, с. 329].

Діяння вважається кримінальним правопорушенням у свідомості людини, коли воно викликає спротив та моральне презирство, а це не обов'язково відбувається в момент закріплення його у кримінальному законодавстві. Тому першочерговим кроком у регулюванні відносин в мережі має бути мінімізація природної латентності стосовно кіберзлочинів у свідомості населення. Ще одним можливим заходом для протидії кіберзагрозам є створення національного Інтернету, хоча це має протиріччя у різних соціальних колах. Проте утворення суверенітету у інформаційному просторі, об'єднання операторів національного сегменту, навпаки, може зробити Інтернет більш уразливим, громіздким і нестійким. У випадку відмови мережі монооператора вся країна може залишитися

без зв'язку. Крім того, буде складно утримувати баланс між безпекою приватних даних конкретної особи, загальнодержавною безпекою і правом на вільний доступ до інформації. Більше того, поява 5G технологій (сателітів зв'язку SpaceX) майже виключає можливість створення закритого кіберпростору. Крім того, утримувати потенційну систему надзвичайно складно і матеріально неекономічно. Таким чином, цілком доцільним є стандартизування міжнародних норм для уникнення міжрегіональних конфліктів.

Для доведення вказаних висновків та тверджень у жовтні 2021 року було виконано практичне кримінологічне дослідження. Під час цього дослідження було опитано 109 респондентів за пілотною програмою, що містила 20 запитань щодо сприйняття українцями цифрових загроз. Отримані результати щодо рівня загальної інтернет-грамотності сучасних користувачів виявилися досить репрезентативними. Дослідження включало аналіз 6 вікових груп: 10–15 років (10,1 %), 16–18 років (15,6 %), 19–25 років (56,9 %), 26–45 років (10,1 %), 46–60 років (5,5 %), 61–99 років (1,8 %). Як очікувалося, найбільш активною групою виявилася 19–25 років, а найменш активною – 61–99 років. У відповідь на запитання «Чи готові ви повністю відмовитися від використання піратських сервісів?» 20,2 % опитаних відповіли «так», 35,8 % – «ні», 22,9 % – «не можу сказати напевне», 21,1 % – «частково». Цікавим для аналізу є віковий розподіл відповідей на це запитання. Більшість респондентів у віці 10–15 років готові відмовитися від піратських сервісів. Це покоління не мало досвіду популярності таких сервісів, сайтів, неліцензійних ігор, контрафактних фільмів. Підлітки вже використовують стрімінгові сервіси, платні підписки, онлайн-кінотеатри та інше, розуміючи, що медіафайли в інтернеті потрібно оплачувати, як і будь-який інший товар.

У віковій категорії 16–18 років 53 % респондентів вибрали варіант «ні», у кожної по 23,5 % були відповіді «не можу сказати напевне» і «частково», в той час як жоден респондент не обрав відповідь «так». У групі 19–25 років 24 % відповіли «так», по 21 % – «не можу сказати напевне» і «частково», тоді як 34 % відповіли «ні». Щодо осіб віком 26–45 років, вони відповіли наступним чином: «так» – 27 %, «не можу сказати напевне» – 27 %, «частково» – 18 %, «ні» – 27 %. У відношенні до дорослих представників цих трьох груп можна зазначити, що їх дорослішання припало на період занепаду, розквіту та становлення піратської ери в Інтернеті. Це пояснює той факт, що більшість у кожній з цих вікових категорій або взагалі не

готові відмовитися від використання піратських джерел, або розглядають лише обмеження його використання. Особливо варто відзначити, що найвищий відсоток повної неготовності виявлено серед наймолодшої групи. Це може бути пов'язано з їхньою віковою психологією, етапом сепарації від родини і відносною матеріальною нестабільністю.

У групі 46–60 років спостерігається такий розподіл відповідей: «так» – 17 %, «не можу сказати напевне» – 33 %, «ні» – 50 %. Щодо представників вікової групи 61–99 років, важливо відзначити, що останній результат потребує обережного аналізу, оскільки в опитуванні брали участь лише дві особи з цієї найстаршої вікової групи. Залишається актуальним спостереження, що люди у зрілому віці не завжди готові платити за контент, який вони споживають у мережі. Це можна пояснити низьким рівнем їх інтеграції в інтернет-середовище та неоднозначним сприйняттям місцевих правил гри.

Важливо врахувати, що відвідування піратських сайтів та завантаження нелегального контенту може призвести до загроз зараження вірусами та введенням шкідливого програмного забезпечення. Оскільки децентралізований обмін файлами передбачає, що комп'ютер стає сервером для інших користувачів, особи самі перетворюють свої пристрої на архіви різної, не завжди легальної інформації. В цілому, проблема піратства в українському сегменті Інтернету є надзвичайно актуальною. Історія «EX.UA», поширеність неліцензійних програм (зокрема, в закладах освіти тощо) представляє собою окремий культурний феномен.

У відповідь на запитання «Чи вважаєте ви себе інтернет-грамотними?», 18,3 % респондентів відповіли «ні», 67 % – «більше так, ніж ні», та 14,7 % – «відмінно знаю, як безпечно користуватись мережею». Щодо запитання «Чи вважаєте ви інтернет-загрози провідною небезпекою сучасності?», 45 % відповіли «так», 9 % – «ні», та 46,8 % – «існують більш важливі проблеми». Між респондентами розбіжні погляди. Суттєва частина опитаних не вважає кіберзлочинність основним викликом XXI століття, тоді як інші вбачають інтернет-загрози як ключові небезпеки. Такий розподіл поглядів наочно демонструє різноманітність державної політики, орієнтованої на багато напрямків, і необхідність її більшої комплексності.

У відповідності з опитуванням, поняття «програміст», «хакер», «розробник» віднесли до одного синонімічного ряду 9,2 %

опитаних; 6,4 % вважають, що лише «програміст» та «хакер» є синонімами; 84,4 % респондентів відзначили, що ці поняття мають різне значення. Такі результати пов'язуються із стрімким розвитком ринку ІТ-послуг. Також слід зазначити, що провідну роль в опитуванні відіграла працездатна молодь, яка завжди зацікавлена в інноваціях та їх створенні.

Аналіз запитань та відповідей свідчить про ставлення до явища хакерства. У запитанні «Ваше ставлення до «професії» хакера» відзначено, що 13,8 % відповіли позитивно, 4,6 % – надзвичайно позитивно, 29,4 % – негативно, 8,3 % – вкрай негативно, а 44 % – нейтрально. При цьому 62,4 % громадян виражають певну схваленість або утримуються від явного відмову від засудження, обираючи нейтралітет. Це свідчить про розуміння певного негативного забарвлення хакерської діяльності, але багато людей відносяться до неї обережно.

Для оцінки інтегрованості населення до кіберпростору були поставлені запитання про зв'язок професійної діяльності з Інтернетом та уподобання в онлайн-покупках. Зокрема, 33 % опитаних пов'язують свою професійну діяльність з Інтернетом, 38,5 % – опосередковано, і лише 28,4 % не мають зв'язку з Інтернетом у роботі. Щодо покупок, 57,8 % респондентів поділили свої уподобання між онлайн та офлайн, 30,3 % віддають перевагу офлайн-магазинам, а 11,9 % переважно купують онлайн. Отже, більшість опитаних працює в Інтернет-сфері або активно використовує його для роботи. Додатково, майже 70 % здійснюють покупки онлайн, що свідчить про високу активність громадян у здійсненні операцій в Інтернеті, особливо в плані розрахункових операцій.

Наступні запитання вказують на рівень усвідомлення проявів невідповідної поведінки у віртуальному середовищі та розуміння основних моделей поведінки в Інтернеті. Під запитаннями «Які з наступних можливостей є порушенням безпеки в інтернеті?» були наведені такі варіанти та відсотки відповідей: «створення акаунту у соціальній мережі від імені іншої особи» – 52,3 % усіх опитаних; «публікація неправдивої або компрометуючої інформації про інших осіб» – 68,8 %; «оприлюднення особистої інформації про людину без її згоди» – 85,3 %; «анонімне або грубе спілкування з іншими особами в Інтернеті» – 33,9 %. Незважаючи на те, що всі ці аспекти

є формами невідповідної поведінки, лише невелика кількість опитаних обрала всі можливі варіанти.

У запитанні «Які з тверджень вважаєте актуальними?» наведені такі варіанти та відсотки відповідей: «анонімність в Інтернеті є абсолютною» – 5,6 %; «персональні дані повністю захищені» – 17,8 %; «персональні дані можуть бути розкриті у випадках загрози національній безпеці для захисту інших осіб» – 42,1 %; «свобода дій в Інтернеті є абсолютною» – 13,1 %; «не погоджуюсь з жодним твердженням» – 40,2 %. Незважаючи на задовільні показники, більшість осіб не повністю розуміють свої права та обов'язки щодо взаємодії з кіберпростором та переоцінюють рівень захищеності своєї приватної інформації.

Для оцінки готовності людей реагувати у складі громадянського суспільства чи самостійно протидіяти негативним явищам в інтернет-середовищі було поставлено таке запитання: «Як ви реагуєте, якщо бачите неприйнятний вміст у мережі (наприклад, шахрайство, цькування, незаконне використання об'єктів права інтелектуальної власності інших осіб)?»: «повідомлю службу підтримки у випадку шахрайства» – 20,2 %; «повідомлю, якщо це цькування» – 7,3 %; «повідомлю, якщо це порушення інтелектуальної власності» – 0,9 %; «повідомлю у всіх випадках» – 43,1 %; «ігноруватиму подібний вміст» – 28,4 %. Громадяни проявили високий рівень готовності протидіяти порушенням в інтернеті. Проте більшість готова повідомляти лише про випадки шахрайства, і значна кількість проявляє байдужість.

Існує очевидний зв'язок між відповідями на такі запитання: 1) «Чи мали ви досвід зустрічі з інтернет-шахраями?», 2) «Якщо відома особа просить вас перейти за посиланням (для участі в опитуванні, конкурсі тощо), ви: ...», 3) «Якщо відома особа просить вас здійснити грошовий переказ, ви: ...». Особи, які особисто відчули негативні наслідки кіберзлочинів, більш обережно ставляться до своєї безпеки в мережі. Таким чином, перше запитання мало наступні результати: «так» – 48,6 %; «особисто ні, але я знаю про такий негативний досвід членів родини, друзів, колег» – 41,2 %; «ні» – 10,1 %. Фактично майже кожен з опитаних повідомив, що особисто чи хтось із його оточення стикався з кіберзлочинами. Щодо другого запитання, то «зробити це, але спочатку дізнатися про деталі» обрали 71,6 %; «проігнорувати» – 11,9 %; «відразу виконати прохання, не розглядаючи деталі» – 16,5 %. Щодо третього запитання: «зробити це, але спочатку дізнатися про деталі» – 63,3 %;

«проігнорувати» – 31,2 %; «все залежить від суми переказу: якщо невелика, то без зволікань відправити» – 5,5 %. Проте варто обдумати такий аспект: близько 5 % осіб проігнорували нашу пропозицію про пройдення опитування, а лише 2 % зацікавилися додатковими деталями щодо дослідження. Це становить велику проблему в контексті зростання кількості випадків зламу акаунтів у соціальних мережах. Майже кожен з нас готовий відреагувати на прохання про допомогу від близької особи, а зловмисники нерідко використовують ці щири відчуття. Посилання на «опитування», конкурси, розіграші призів і подібне можуть бути вірусними або переадресовувати на сторінку-дублікат, яка збирає особисті дані (паролі, банківські картки).

Цікаво відзначити, що як особи, що вже мали досвід зіткнення з шахрайством в мережі, так і ті, хто не мав такого досвіду, високо не оцінили ефективність дій державних установ у запобіганні цифровим загрозам. На запитання «Як ви оцінюєте здатність державних структур за п’ятибальною шкалою захистити ваші права в Інтернеті?» відповіли так: 1 бал – 30,3 %; 2 бали – 33 %; 3 бали – 26,6 %; 4 бали – 9,2 %; 5 балів – 0,9 %. Отже, державним органам потрібно зосередити увагу не лише на відповідному технічному забезпеченні та підготовці кадрів, але й на розробці ефективної маркетингової стратегії для створення позитивного іміджу перед громадськістю.

Отже, розглянувши наукові праці та дані офіційної статистики можна сформулювати типовий кримінологічний портрет особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій:

– більшість підозрюваних за кримінальні правопорушення у сфері інформаційних технологій, які перебувають у міжнародному розшуку, – це чоловіки віком 20–35 років, значна кількість таких злочинців є громадянами держав, в яких присутній низький рівень протидії кіберзлочинам (країни Середнього, Далекого Сходу).

– більшість громадян України, які були підозрюваними за вчинення кримінальних правопорушень у сфері інформаційних технологій, також були особами чоловічої статі, але кримінальні провадження за кібершахрайство відкривались також і щодо жінок та за співучастю особами чоловічої та жіночої статі;

– більше половини підозрюваних злочинців мали вищу освіту, інші мали середньо-спеціальну та середню освіту;

– більшість кібершахраїв самостійно отримують освіту та досвід у сфері високих інформаційних технологій (комп'ютерної безпеки, програмування тощо) поза закладом освіти, без педагогічної допомоги, це зумовлює, що особи кіберзлочинців здебільшого мають спеціальні технічні знання [42].

2.4. Класифікація кримінальних правопорушень у сфері інформаційних технологій

Відповідно до сучасної доктрини міжнародного кримінального права, кримінальні правопорушення, які використовують комп'ютерні технології (відомі як «кіберзлочини»), вважаються кримінальними правопорушеннями міжнародного характеру. Перелік кіберзлочинів визначений у Конвенції про кіберзлочинність (2001 р.), серед яких зазначені такі:

– незаконний доступ до комп'ютерної системи,

– нелегальне перехоплення технічними засобами комп'ютерних даних,

– втручання у комп'ютерні дані,

– втручання у функціонування комп'ютерної системи,

– підробка та шахрайство, пов'язані з комп'ютерами,

– порушення, пов'язані з дитячою порнографією тощо.

У пункті 14 Доповіді Комітету II Десятого Конгресу ООН 2000 р. щодо запобігання злочинності та поводження з правопорушниками зазначено, що існують дві категорії кримінальних правопорушень:

1. Кіберзлочини в їх тісному розумінні (також відомі як «комп'ютерні» злочини) представляють собою будь-які незаконні дії, які виконуються за допомогою електронних операцій з метою проникнення у захищені комп'ютерні системи та їх оброблювані дані.

2. Кіберзлочини в їх широкому розумінні (також відомі як злочини, пов'язані з використанням комп'ютерів) охоплюють будь-які незаконні дії, які вчиняються у зв'язку з комп'ютерними системами або мережами, включаючи незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [86, с. 338].

Варто зазначити, що Конвенція про кіберзлочинність визначає кримінальну відповідальність за кіберзлочини як у вузькому, так і в широкому розумінні. Проте кримінальне законодавство окремих

країн світу, така як Україна, визначає кримінальну відповідальність за кіберзлочини лише в вузькому розумінні. В Особливій частині Кримінального кодексу України існує розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Проте жодна зі статей цього розділу не передбачає можливість притягнення особи до відповідальності за кіберзлочини в широкому розумінні, наприклад, шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК) або інших суспільно небезпечних дій, передбачених ст. 200 КК. На думку А. А. Музики та Д. С. Азарова, і цей підхід можна підтримати, використання комп'ютерів для вчинення таких дій є лише конкретним методом вчинення кримінального правопорушення, який зазвичай не включається до обов'язкових ознак об'єктивної сторони складу кримінального правопорушення. У випадку наявності певних фактичних обставин, ці кримінальні правопорушення можуть бути кваліфіковані як сукупність кримінально протирпавних діянь, передбачених Розділом XVI Особливої частини Кримінального кодексу України [206]. Потрібно також зауважити, що завдяки застосуванню комп'ютерних технологій значна кількість «звичайних» кримінальних правопорушень перейшла сьогодні до категорії «кіберзлочинів». До того ж, способи їх вчинення істотно полегшились, а «географія» розширилась. До таких кримінальних правопорушень, що перейшли з реального, фізичного світу до кіберпростору, можна назвати тероризм, розповсюдження порнографічної інформації, відмивання грошей тощо [342].

Дослідники вказують, що «кіберзлочини» мають низку характеристик, які дозволяють їм впливати на міжнародний правопорядок через комп'ютерні системи, зокрема – на міжнародний обмін інформацією. Сьюзанн В. Бреннер виділяє такі особливості кіберзлочинів, які відрізняють їх від «звичайних» кримінально протиправних посягань і значно підвищують їх суспільну небезпечність. По-перше, «кіберзлочин» не потребує фізичного контакту між жертвою та злочинцем у момент вчинення. По-друге, «кіберзлочин» є «автоматизованим» кримінальним правопорушенням, оскільки суб'єкт кримінального правопорушення, використовуючи комп'ютерні технології, може за короткий період збільшити кількість протиправних дій до декількох тисяч. По-третє, суб'єкт «кіберзлочину» не обмежений обмеженнями, що існують у

реальному, фізичному світі. Так, «кіберзлочини» можуть бути вчинені миттєво і, отже, вимагають швидкої реакції. І вчетверте, «кіберзлочинність» є новим явищем, і наука поки не в змозі визначити моделі поширення різних видів кримінальних правопорушень з географічною та демографічною специфікою, як це відбувається зі протиправними правопорушеннями, що відбуваються у реальному, фізичному світі [363]. Поза кримінологічними аспектами, які досліджувала ця авторка, існує низка інших правових питань, які ще не мають чіткого врегулювання. Однією з них є визначення місця вчинення кримінального правопорушення через Інтернет. Наприклад, яке право країни слід застосувати, якщо кримінальне правопорушення та його об'єкт перебувають у різних країнах? Як вирішити питання про можливі та необхідні межі застосування кримінального закону країни до «кіберзлочинів», вчинених за її межами?

Аллан Р. Стейн, зокрема, наголошує, що найбільш проблемною характеристикою Інтернету з юрисдикційної точки зору є те, що він стирає межу між внутрішньодержавною і міжнародною передачею інформації. [393]. Інтернет виник і є засобом міжнародного спілкування та обміну інформацією, який діє в межах віртуального простору та не підкоряється централізованому керівництву.

Кожна особа та її комп'ютер діють автономно, утворюючи єдину глобальну мережу, яка виходить за межі географічних кордонів країн. Інтернет-адреси, підтримувані цією мережею, є нематеріальними, і навіть URL-адреси, які містять індикатори країни походження, такі як «ua», «pl», можуть бути неточними.

Адреси Інтернет є гнучкими і можуть залишатися незмінними, навіть коли сервери фізично переміщуються [11, с. 24–31]. Ця характеристика Інтернету вимагає від науки та практики розробки нових стратегій для протистояння міжнародним кіберзлочинам та створення ефективної юрисдикційної політики щодо цих противоправних дій.

Існує кілька основних способів вирішення цього завдання та подальшого регулювання Інтернету та кримінальної відповідальності за міжнародні кіберзлочини. За першим з них рекомендується адаптувати традиційні принципи кримінальної юрисдикції до кримінальних правопорушень, які вчиняються за допомогою сучасних інформаційних технологій. Щодо другого напрямку, пропонується розглядати Інтернет як окремий «віртуальний» кіберпростір та розробляти нові правила застосування кримінальної

юрисдикції для кримінальних правопорушень, що відбуваються у цьому середовищі.

Прибічники першого підходу стверджують, що нові технології Інтернету автоматично не впливають на правову доктрину кримінальної юрисдикції, і ці принципи можна застосовувати до «кіберзлочинів» міжнародного характеру. Вони вказують на те, що правові підстави для цих дій передбачені, як вони стверджують, у Конвенції про кіберзлочинність (2001 р.). Справді, Конвенція визначає традиційну схему кримінальної юрисдикції для регульованих кримінальних правопорушень, враховуючи територіальний та національний принципи кримінальної юрисдикції. Частина перша статті 22 Конвенції закріплює, що кожна з Сторін приймає такі законодавчі й інші заходи, які, на її думку, можуть бути необхідними для встановлення юрисдикції у відношенні будь-якого злочину, що криміналізований за Конвенцією, якщо він вчинений:

a. на її території;

b. на борту судна, яке плаває під прапором такої Сторони, або

c. на борту літака, зареєстрованого відповідно до законодавства такої Сторони, або

d. одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої Держави.

Проте Конвенція не надає визначення того, які «кіберзлочини» слід вважати вчиненими на території конкретної країни, або що розуміти під поняттям «місце вчинення злочину», залишаючи це на розсуд національних судів. Міжнародний досвід показує, що національні правові системи мають різні підходи до вирішення цього питання. Розбіжні трактування місця вчинення кримінальних правопорушень, пов’язаних з комп’ютерними технологіями, та відсутність чіткого правового регулювання на міжнародному рівні можуть спричинити, з одного боку, позитивні конфлікти міжнародних кримінальних юрисдикцій різних країн, коли дві або більше країни претендують на застосування своїх законів щодо кримінальної відповідальності за одну й ту ж кримінально протиправну дію. З іншого боку, це може призвести до негативних конфліктів міжнародних кримінальних юрисдикцій, коли жодна країна не вживає заходів щодо переслідування вчиненого кримі-

нального правопорушення. У міжнародній правозастосовчій практиці питання кримінальної юрисдикції залежить від існуючого поділу кіберзлочинів за колом об'єктів:

– кримінальні діяння, спрямовані на конкретні об'єкти та завдають їм шкоду (наприклад, банківській установі, особистій електронній пошті тощо);

– кримінальні діяння, спрямовані на невизначене коло об'єктів та завдають їм шкоду (наприклад, поширення комп'ютерних вірусів, порнографічних матеріалів тощо).

Вирішення питання про застосування кримінального закону держави до «кіберзлочинів», які спрямовані на конкретні об'єкти, часто ґрунтується на принципах об'єктивної територіальності. Індивід, перебуваючи в одній країні, вчиняє кримінально протиправну дію, спрямовану на територію інших юрисдикцій, використовуючи сучасні комп'ютерні мережі. Правоохоронні органи країни, де він знаходиться фізично, часто навіть не мають поняття про його кримінальну діяльність, і виявляють це тільки за наслідками, що виникають в іншій країні. У таких ситуаціях кримінальне переслідування злочинця може бути неможливим без міжнародного співробітництва. Правопорушник підлягає відповідальності на території країни, де він перебуває, або може бути видача до «потерпілої» країни за наявності відповідних міжнародних договорів та дотримання інших правових умов, що супроводжують процедуру екстрадиції (принцип подвійної кримінальності, виключення видачі власних громадян тощо). Однак екстрадиційна процедура є складною та, скоріше, винятковою, а не загальним методом вирішення схожих питань.

Міжнародний досвід також показує особливі ситуації, коли «потерпіла» країна вирішує притягнути злочинця до кримінальної відповідальності без звернення до країни його перебування. Наприклад, у 2000 році громадянин російської федерації О. Іванов здійснив «хакерську атаку» на систему захисту корпорації з електронної комерції, що розташована в штаті Коннектикут, США. Він отримав ключові паролі доступу та контролю над усією системою та погрожував знищити всю комп'ютерну мережу корпорації, якщо не отримає пропозицію про працевлаштування на посаду експерта з безпеки. О. Іванова запросили на співбесіду до США, де він був заарештований та підданий судовому розгляду. На судовому засіданні О. Іванов намагався довести, що суд США не має

компетенції стосовно вчиненого ним кримінального правопорушення, оскільки в момент «хакерської атаки» він перебував на території іншої країни. Суд відкинув ці аргументи та у своєму рішенні вказав, що О. Іванов намагався завдати шкоду території США своїми діями, хоча перебував поза її межами під час здійснення кримінально протиправного наміру, і використав статут, який не мав прямого зовнішнього застосування [342].

Ситуація із застосуванням кримінальної юрисдикції до «кіберзлочинів», що націлені на різноманітні об'єкти та порушують правопорядок у багатьох країнах, має свої особливості. У цих випадках можливе притягнення особи до кримінальної відповідальності на засадах екстериторіальності, з попередженням, за умови, що в країні існує кримінальна заборона щодо «кіберзлочинів».

За цією інформацією можна зробити висновок, що сучасні країни надалі застосовують традиційні принципи кримінальної юрисдикції до «кіберзлочинів» та «комп'ютерних злочинів», ґрунтуючись на концепції географічної територіальності. Проте оскільки сучасні комп'ютерні мережі функціонують поза межами територіального суверенітету та є позатериторіальними за своєю природою, традиційні принципи кримінальної юрисдикції часто стають неефективними та породжують численні правові питання.

Але існує альтернативний підхід до регулювання правових відносин в мережі Інтернет, який може бути більш адаптованим до сучасності. Прихильники цього підходу пропонують вважати місцем вчинення «кіберзлочину» сам кіберпростір, а не територію конкретної країни або будь-яку іншу географічну область.

Верховний Суд США запропонував таке визначення кіберпростору: «Це унікальний носій, який не має конкретної території, але доступний кожному в будь-якій точці світу через Інтернет».

Погоджуємося з тим, що доречніше кримінальну юрисдикцію кіберзлочинів не асоціювати з певною територією, щоб не виникали суперечності між країнами. Юрисдикцію таких кримінальних правопорушень потрібно розширити до кіберпростору і напрацювати один єдиний підхід до кваліфікації таких діянь та їх розслідування.

Інституціональним втіленням кіберпростору є Інтернет – глобальна інформаційна система, яка складається з інших інформаційних систем і дозволяє користувачам обмінюватися інформацією з будь-

яким комп'ютером у цій системі [355]. Досить логічно, враховуючи вищезазначене, надати Інтернету правовий статус, аналогічний територіям загального користування (космічний простір, відкрите море, Антарктида тощо). Це відкриє можливість застосовувати відповідальність за правопорушення в кіберпросторі згідно з принципами кримінальної юрисдикції, які діють в інших територіях загального користування. Іншими словами, особа, яка вчинила кримінальне правопорушення у кіберпросторі, понесе відповідальність перед країною свого громадянства.

Зазначене правило може вступити в силу лише за умови прийняття всеагентного набору правил користування Інтернетом та впровадження принципу обов'язкового співробітництва між країнами у розслідуванні злочинів, вчинених у кіберпросторі.

Дещо спірна думка науковців стосовно того, що відповідальність за вчинення кримінальних правопорушень в кіберпросторі особа повинна нести перед країною свого громадянства, тому що в деяких країнах не передбачено відповідальності за такі правопорушення. В такому випадку протиправні діяння особи залишаться безкарними. Щоб цього уникнути, потрібно передбачити єдиний механізм щодо притягнення до відповідальності кіберзлочинців. Наприклад, якщо в певній країні не передбачено покарання за такі кримінальні правопорушення, то в такому разі застосовувати єдиний механізм притягнення до відповідальності.

До того, як будуть прийняті відповідні правові акти, правоохоронні органи та суди України, що займаються розслідуванням та розглядом справ про міжнародні кіберзлочини, повинні враховувати наступні критерії, які обґрунтовують доцільність застосування кримінальної юрисдикції:

– можливе настання серйозних суспільно небезпечних наслідків для інтересів держави або громадян;

– зв'язок з суб'єктом кримінального правопорушення (національність, місце постійного проживання);

– пов'язаність злочину та злочинця з територією країни;

– відповідність правил кримінальної юрисдикції чинним нормам міжнародного права та міжнародним зобов'язанням держави;

– юридичні підстави для застосування кримінальної юрисдикції іншою державою та ймовірність конфлікту кримінальних юрисдикцій.

Аналізуючи історичний аспект «кіберзлочинів», важливо згадати, що їх початок мав місце в Америці, коли у 1945 році була створена перша електронно-обчислювальна машина (комп'ютер), яка використовувалася для дешифрування німецьких військових кодів, а пізніше й з іншими цілями. Сучасно ця тенденція також спостерігається, коли суперкомп'ютери та мережеві системи багатоцільового використання в основному використовуються для розв'язання завдань забезпечення інформаційної безпеки, а потім вже для інших локальних цілей.

З поширенням комп'ютерної техніки у різних країнах світу стали розповсюдженими випадки кримінальних правопорушень, що використовують комп'ютери та передові інформаційні технології. Це не залишило байдужими криміналістів-практиків і науковців, які усвідомили реальну загрозу національній безпеці своїх держав та передбачили негативні глобальні наслідки для технологічно розвинених країн та інформаційного світу в цілому.

Починаючи з 1958 року, правова статистика Стенфордського дослідницького інституту характеризує такі види «комп'ютерних» кримінальних правопорушень у XX столітті:

– випадки пошкодження та крадіжки комп'ютерного обладнання, а також незаконне копіювання інформації;

– шахрайство або відмивання грошей, здійснені за допомогою комп'ютерів;

– несанкціоноване використання комп'ютерів або незаконне використання машинного часу.

У 1966 році був зафіксований перший випадок використання ЕОМ як інструмента під час пограбування банку в Міннесоті. Першою особою, яка скористалася ЕОМ для вчиненння податкового кримінального правопорушення на суму 620 тисяч доларів і стала перед американським судом у 1969 році, був Альфонсо Конфессоре.

Подальша історія «комп'ютерних» злочинів відмічена такими найбільш «яскравими» подіями:

– кінець 70-х – пограбування «Секьюріті пасифік банк» (10,2 млн. доларів);

– 1979 р. – комп'ютерне розкрадання у Вільнюсі (78584 крб.);

– 1984 р. – повідомлення про перший в світі «комп'ютерний вірус»;

– 1985 р. – виведення з ладу за допомогою «вірусу» електронної системи голосування в конгресі США;

– 1986–1988 рр. – поява першого «комп'ютерного вірусу» в СРСР;

– 1989 р. – блокування американським студентом 6000 ЕОМ Пентагону;

– 1990 р. – міжнародний з'їзд комп'ютерних «піратів» у Голландії з демонстрацією можливості необмеженого втручання в системи ЕОМ;

– 1991 р. – розкрадання коштів Зовнішекономбанку на суму в 125,5 тис. доларів;

– 1992 р. – умисне порушення роботи АСОВІ реакторів Ігналінськой АЕС;

– 1993 р. – електронне шахрайство в Центробанку Росії (68 млрд. крб.);

– 1995 р. – спроба російського громадянина пограбувати Сіті-банк на суму 2,8 млн. доларів.

Початок XXI століття відзначився широким поширенням комп'ютеризованих (автоматизованих) інформаційно-технологічних систем на міжнародному рівні у виробничій, комерційній, банківській та інших галузях. Це привело до необхідності термінового розроблення ефективної системи захисту цих систем від несанкціонованого доступу. Ця проблема стала надзвичайно актуальною відповідно до зростання обсягу інформації, що обробляється згаданими інформаційно-технологічними системами, особливо завдяки інтенсивному розвиткові глобальної комп'ютерної мережі Інтернет.

Україна також не залишилася осторонь розвитку комп'ютерної інфраструктури. Національні фінансові установи та інші юридичні та фізичні особи відкрили доступ до міжнародних платіжних систем, електронної комерції, різних міжнародних проєктів і програм, таких як дистанційна освіта, наукові дослідження та інше. Кількість користувачів Інтернету перевищила мільйонну межу.

Одночасно з позитивними наслідками набули популярності та поширення численні недоліки, які можна розглядати як негативний аспект технологічного прогресу. Швидкими темпами розрослися кримінальні правопорушення, використовуючи можливості комп'ютерної мережі Інтернет та сучасні комп'ютерні технології. З'явилися нові кваліфіковані форми злочинів, такі як «кібертероризм», «кібершахрайство», «кіберрозкрадання», «кіберпорнографія» та інші.

Характер цих кримінально протиправних не вимагає або довготривалої підготовки, або значного часу для втілення незаконних намірів. Розповсюдженість у географічному плані, віддаленість об'єктів атаки (на тисячі або сотні тисяч кілометрів від місця вчинення кримінального правопорушення), труднощі у виявленні та доведенні вини, а також високий рівень прибутковості роблять цей вид кримінально протиправної діяльності особливо привабливим для злочинців.

Згідно з даними Інтерполу, представленими на Шостому засіданні Робочої групи щодо співпраці правоохоронних органів країн Центральної та Східної Європи у серпні 2000 року з питань боротьби з «кіберзлочинністю», доходи злочинців, пов'язані з незаконним використанням сучасних технологій, займають третє місце у світі після доходів від торгівлі наркотиками та зброєю.

За повідомленням агентства Reuters, обсяг грошей, що були викрадені та вимагалися «кіберзлочинцями» у 2004 році, склав 105 мільярдів доларів США. Американські експерти прийшли до висновку, що середній збиток від одного «кіберзлочину» в США становить 500 тисяч доларів, тоді як вартість одного фізичного пограбування банку оцінюється у 3,2 тисячі доларів. За даними ФБР, щомісяця американські бази даних стають об'єктом понад тисячі атак з боку іноземних хакерів.

Збитки від одного «кіберзлочину» на Заході у середньому коливаються від 450 тисяч до 1 мільярда доларів США. Щорічні втрати для компаній США становлять 100 мільярдів доларів, для Великобританії – 4,45 мільярда доларів, а для країн Західної Європи – 39 мільярдів доларів.

Згідно з соціологічним опитуванням, проведеним Інститутом комп'ютерної безпеки та ФБР, 57 % організацій-респондентів вважають комп'ютерну мережу Інтернет місцем організації та реалізації небажаних інформаційних та електронних атак, 30 % вбачають її як джерело несанкціонованого проникнення до своїх комп'ютерних мереж сторонніх осіб, а 26 % заявили про факти крадіжки інформації з обмеженим доступом та приватного характеру через Інтернет.

Не випадково ще у 1992 році, кримінально протиправні діяння у цій сфері були включені Організацією Об'єднаних Націй до списку 14 видів транснаціональних злочинів, порівнявши їх з «відмиванням» грошей, терористичною діяльністю, організованим

наркобізнесом, крадіжкою витворів мистецтва, порушенням інтелектуальної власності, незаконною торгівлею зброєю, захватом повітряних суден, морським піратством, заволодінням наземного транспорту, шахрайством, екологічними злочинами, торгівлею людьми, торгівлею людськими органами та тканинами.

Питання «кіберзлочинності» було детально висвітлено на першому міжнародному стратегічному Конгресі «E-Crime Congress 2002», який відбувся у Лондоні у грудні 2002 року. Ініціатором та організатором цього Конгресу виступила Національна управління боротьби з кримінальними правопорушеннями у сфері високих технологій (National Hi-Tech Crime Unit – NHTCU) – перша національна правоохоронна організація Великобританії, яка мала за мету боротьбу з «комп'ютерною» злочинністю та співпрацю з іншими правоохоронними структурами. У роботі конгресу «E-Crime» було близько 400 делегатів, включаючи представників Австралії, Нової Зеландії, Кореї, Гонконгу, Латвії та США, які представляли як державні, так і недержавні організації, які займалися питаннями захисту інформації та розслідуванням комп'ютерних злочинів. Серед учасників були представники МВС Великобританії, Інтерполу, ФБР, Microsoft, Symantec, IBM, Sun Microsystems Ltd., VISA, MasterCard, eBay, Bank of New York та Swedbank.

На Конгресі було підкреслено, що високотехнологічна злочинність, особливо в організованих формах, стрімко зростає, переважно через вплив глобальної мережі Інтернет. Факт перебування в Інтернеті дозволяє порушувати закон незалежно від громадянства та місця перебування, маніпулювати та обманювати людей, а також приховувати докази і вкрадену інформацію. Ці дії становлять значну небезпеку для критичних інфраструктур країн світу, включаючи економічну, екологічну та військову безпеку, про що свідчать дані, що були представлені в одній з доповідей учасників Конгресу.

Лише у США 90 % організацій щорічно виявляють порушення в інформаційних системах (у жовтні 2002 року, кібератака, що тривала годину, призвела до відмови 9 з 13 основних комп'ютерів керівників глобального руху в мережі Інтернет); 80 % організацій підтверджують фінансові збитки (тільки один вірус NIMDA спричинив матеріальні збитки понад 1,8 млрд. фунтів); щорічно стають свідками крадіжок приватної інформації на суму понад 38 млрд. фунтів.

Прогнозування такого розвитку ситуації спонукало до розробки та впровадження ефективних засобів протидії. Першочергово, ці заходи базувались на досягненнях у галузі кримінального права та криміналістики, а також на глибоких наукових дослідженнях міжнародного та національного рівнів.

Будапештська Конвенція (Конвенція про кіберзлочинність) упорядкувала кіберзлочини на п'ять груп. Початково було класифіковано їх у чотири групи, але пізніше був прийнятий Додатковий протокол, розширюючи класифікацію.

Перша група включає кримінальні правопорушення, що порушують доступність, конфіденційність та цілісність комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в систему та дані). Друга група охоплює кримінальні правопорушення, пов'язані з використанням комп'ютера як інструмента для вчинення кримінальних правопорушень (маніпуляції з інформацією), такі як комп'ютерне підроблення та комп'ютерне шахрайство. Третя група охоплює кримінальні правопорушення, пов'язані з контентом, зокрема з вмістом даних у комп'ютерних мережах (особливо розповсюджені кримінальні правопорушення, пов'язані з дитячою порнографією). Четверта група стосується порушень авторського права і суміжних прав (визнання порушень, пов'язаних з авторським правом, компетенцією національних законодавств країн). П'ята група кримінальних правопорушень визначена окремим протоколом і стосується актів расизму та ксенофобії, вчинених за допомогою комп'ютерних мереж.

На нашу думку, потрібно виділити ще одну групу кіберзлочинів – кібертероризм (кібервійни), тому що це – єдиний вид кіберзлочинів, який за своєю суттю є дуже потужним та здатен завдавати колосальних збитків не лише окремим структурам чи особам, але і цілій низці країн.

На перший погляд, відмінності кібертероризму (інформаційного тероризму) від класичного тероризму можуть здатися менш наляклівими. Тут немає вибухів, образливих кількостей жертв і проникливих криків поранених. Однак, при докладнішому розгляді виявляється, що ситуація не настільки оптимістична. Інформаційний тероризм включає не лише кіберзлочини, хоча, звісно ж, вони є складовою цього явища. Сюди також входять некоректні маніпуляції

інформацією або її спотворення, а в деяких випадках навіть намагання представити намірено невірні факти, що призводить до залякування населення та поширення параноїдальних поглядів.

Вплив інформаційних кримінальних правопорушень на інформаційну безпеку держави є значущим не лише через значний економічний збиток, спричинений цими кримінальними правопорушеннями. Відразу, перш за все, це через те, що наслідком цих кримінально протиправних діянь є порушення нормального функціонування інформаційних та комунікаційних систем. Також поширюється інформація, що має незаконний характер [348, с. 57].

Серед різноманітних протиправних дій, пов'язаних з інформацією, виділяються певні сукупності, що мають спільну спрямованість і представляють собою видові групи правопорушень у сфері інформаційних відносин:

1. Порушення прав щодо інформації та інформаційних ресурсів, які торкаються інформаційних правовідносин, пов'язаних з забезпеченням відповідних технологічних характеристик інформації (конфіденційності, цілісності, доступності, спостережності).

2. Порушення прав щодо інформаційного простору, які впливають на інформаційні правовідносини, пов'язані з якістю та цінністю інформації (повнота, об'єктивність, своєчасність, безпечність тощо), зокрема належним наданням відповідної інформації, уникненням поширення небезпечної інформації та використанням технологій деструктивного інформаційно-психологічного впливу.

3. Порушення прав щодо інформаційної інфраструктури, що впливають на інформаційні правовідносини, які виникають у сфері використання об'єктів інформаційної інфраструктури (інформаційно-телекомунікаційні системи, комп'ютери, сервери, програмне забезпечення тощо).

4. Інші правопорушення в сфері інформації, для яких характерне використання інформації, інформаційного простору та інформаційної інфраструктури при вчиненні протиправних дій, що торкаються інших правовідносин (щодо приватної власності, суспільної та державної безпеки, господарської діяльності тощо).

Ця класифікація має теоретичний характер і дозволяє розробляти інші теоретичні та специфічні класифікації порушень у сфері інформації, використовуючи відомі ознаки, зокрема:

А) в залежності від ступеня суспільної небезпечності (інформаційні злочини та проступки);

Б) на основі форми зовнішнього вираження (протиправні дії або бездіяльність);

В) залежно від виду юридичної відповідальності (інформаційні правопорушення, за які передбачена кримінальна, адміністративна, цивільно-правова, дисциплінарна та інша відповідальність);

Г) з огляду на галузі діяльності (інформаційні правопорушення у галузі господарської, економічної, політичної, інформаційної діяльності та інше) [231].

Т. Л. Тропіна провела глибокий аналіз кіберзлочинів і пропонувала таку класифікацію:

1. Потенційно небезпечні кіберзлочини, які загрожують фізичній безпеці, здоров'ю і життю людини.
2. Кримінальні правопорушення, що порушують конфіденційність інформації, такі як незаконний доступ до комп'ютерів або комп'ютерних систем без завдання шкоди інформації.
3. Деструктивні кіберзлочини, що полягають у шкоді даним і порушують цілісність та безпеку функціонування комп'ютерних систем.
4. Кримінальні правопорушення, що посягають на майно, майнові права, а також права власності на інформацію і авторські права.
5. Кримінальні правопорушення, що впливають на суспільну мораль.
6. Інші кіберзлочини, такі як «computer-facilitated» (традиційні кримінальні правопорушення, які полегшує або надає нові можливості комп'ютер; цю групу можна розглядати як ті, що включають різноманітні злочини, наприклад: реклама послуг проституції в мережі Інтернет (що є злочином не в усіх країнах), незаконний обіг наркотиків через мережу Інтернет, азартні ігри в Інтернеті (також не завжди кримінально карні), відмивання коштів через електронні трансакції, кіберконтрабанда, тобто передача незаконних товарів через Інтернет, таких як заборонені в деяких країнах шифрувальні технології та інше).

Більшість кримінальних правопорушень, які відбуваються у глобальних комп'ютерних мережах, мають такі характеристики:

– високий ступінь таємниці вчинення кримінального правопорушення, що пояснюється особливостями мережевого інформаційного простору (використання розроблених засобів анонімності, складнощі в структурі тощо);

– транснаціональний характер мережевих кримінальних правопорушень, за якого злочинець, об’єкт злочину та потерпілий можуть знаходитися на територіях різних держав; високий рівень підготовки злочинців, інтелектуальна складова кримінально протиправної діяльності діяльності; нетиповість, складність та постійне оновлення методів вчинення кримінальних правопорушень та спеціальних засобів, що використовуються;

– можливість вчинення кримінальних правопорушень в автоматизованому режимі в кількох місцях одночасно;

– багатоаспектний характер кримінально протиправних дій при численності потерпілих;

– невідомість потерпілих щодо того, що вони стали жертвами кримінально протиправної дії;

– віддалений характер кримінально протиправних дій в умовах відсутності фізичного контакту між злочинцем і потерпілим;

– неможливість передбачення та припинення злочину даного виду за допомогою традиційних засобів [226, с. 4].

Особливу увагу слід зосередити на надзвичайній актуальності вивчення категорії порушень, які взагалі виходять за межі національних юридичних систем та становлять загрозу для всесвітнього співтовариства – «міжнародних інформаційних злочинів». Це кримінально протиправна діяльність представників міжнародної політики, спрямована на відкрите спотворення інформаційного простору шляхом потужної інформаційної експансії, систематичної дезінформації, інформаційної ізоляції окремих регіонів та створення перешкод для міжнародних спостерігачів з метою формування ілюзорної суспільної думки. Ця кримінально протиправна практика не відповідає гуманістичним та правовим ідеалам сучасного суспільства та становить загрозу світовому порядку [310, с. 43].

Міжнародне кримінальне право має розроблені механізми та стратегії для протидії транснаціональним злочинам. Серед них особливе значення має міжнародно-правове регулювання боротьби з кіберзлочинністю, оскільки цей вид злочинності поширюється надзвичайно швидко. Методи та способи вчинення кіберзлочинів постійно вдосконалюються, іноді навіть випереджають засоби захисту комп’ютерної інформації. Згідно з щорічною доповіддю про глобальні виклики, цей вид злочинів має потенціал стрімкого зростання [394],

Згідно дослідження Міжнародної організації «World Economic Forum», яка займається аналізом проблем глобального, регіонального та галузевого співробітництва між державами та приватним сектором, у 2019 році проблеми кібербезпеки та кіберзлочинності посіли четверте та п'яте місця у списку світових загроз. У цьому документі підкреслюється стійке збільшення рівня загроз у всіх сферах суспільства, та передбачається подальше зростання цього виду кримінальних дій у найближчі десять років. Кіберзлочинність є динамічною та постійно еволюціонує, з'являються нові види кримінальних правопорушень, нові концепції, технології розвиваються швидко, і тому необхідно своєчасно підтримувати співробітництво у сфері законодавства.

Організація Об'єднаних Націй, Рада Європи, Європейський Союз, Організація з безпеки і співробітництва в Європі та інші важливі міжнародні організації активно працюють над розробкою стратегій запобігання кіберзлочинності та формуванням спільної політики з утримання цього загрозливого явища. Ця діяльність охоплює організацію міжнародних конгресів, форумів, прийняття конвенцій, резолюцій та інших заходів. Особлива увага до кіберзлочинності, пов'язаної з використанням комп'ютерів, була зосереджена під час Одинадцятого конгресу ООН з попередження злочинності та кримінального правосуддя, який відбувся в Бангкоку, Таїланд, у квітні 2005 року [167].

Це питання було включено до порядку денного і обговорювалось у контексті ефективних заходів запобігання транснаціональній організованій злочинності. Експерти ООН у своїх рекомендаціях перед Одинадцятим конгресом звернули увагу на специфічний характер кіберзлочинності та необхідність використання комплексних підходів у боротьбі з нею. Також було наголошено на необхідності негайних заходів щодо оновлення кримінального законодавства країн-учасниць ООН, включаючи уточнення чи вилучення норм, що втратили актуальність, або прийняття нових норм, що стосуються нових форм кіберзлочинів. Під час конгресу було зазначено: «поширення нових інформаційно-комунікаційних технологій по всьому світу породило безліч різноманітних кримінальних правопорушень, пов'язаних з використанням комп'ютерів, які загрожують не лише конфіденційності, цілісності та доступності комп'ютерних систем, але й безпеці важливих елементів інфраструктури. Крім того, технологічні інновації породжують різні тенденції

у сфері «кримінальної інновації», що відображає розбіжності в загрозах, які несе кіберзлочинність, по всьому спектру так званого «розриву в цифрових технологіях» [167].

Глобальна доступність електронних та віртуальних послуг призводить до того, що злочинність у сфері інформаційного простору має невід'ємний міжнародний аспект. Обмеження міжнародної кіберзлочинності є необхідною складовою національної кібербезпеки та стратегії захисту критичної інформаційної інфраструктури.

Як вказує професор Н. А. Зелінська, «на національному рівні це є спільною відповідальністю, що передбачає скоординовані дії з боку урядових організацій, приватного сектору та громадян. На регіональному та міжнародному рівнях це веде до співпраці та координації зусиль між країнами» [135, с. 467]. Професор В. М. Дрьомін стверджує, що сучасна інформаційна обстановка сприяє виникненню злочинності, і відзначає наявність стійкого системного взаємовпливу в контексті «інформація – злочинність». Розвиток інформаційного мегасередовища має значний вплив і призводить до глобалізації злочинності, що стрімко набуває поширення. Незважаючи на різницю у внутрішньому характері цих соціальних явищ, спостерігається міцна взаємозалежність та тенденція до її зміцнення [121, с. 54].

Варто зазначити, що в наш час немає ні достатньо репрезентативної статистики, що відображала більш точну картину ситуації зі злочинністю у сфері інформаційних технологій, ні надійних методів збору відповідних даних. Крім того, відсутня єдиність в національному кримінальному законодавстві країн у сфері боротьби з злочинністю у сфері інформаційних технологій.

Міжнародні документи, зокрема Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті», прийнята 12 грудня 2003 року, підкреслює необхідність розвитку міжнародного співробітництва в сфері інформаційного простору для запобігання кіберзлочинам [114]. У Женеві відбувся перший етап Всесвітньої зустрічі на вищому рівні, в якій взяли участь представники народів світу. Також важливі міжнародні ініціативи в сфері інформаційного суспільства включають «Окінавську Хартію глобального інформаційного суспільства», прийняту 22 липня 2000 року країнами «Великої вісімки», а також

Туніську програму для інформаційного суспільства, затверджену у 2005 році. ЮНЕСКО ухвалило Програму «Інформація для всіх» в 2001 році. Міжнародні нормативно-правові акти, які мають універсальний та регіональний характер, складають правову основу у боротьбі з кіберзлочинністю. Одним із таких актів є Конвенція ООН проти транснаціональної організованої злочинності, що була прийнята 15 листопада 2000 року [163]. У зазначеному документі відображені основні напрямки міжнародного співробітництва у цій сфері. Наголошено, що кіберзлочини мають транснаціональний характер і можуть спричинити значну шкоду економічному розвиткові країн. Зокрема, вчені вказують, що «несумнівно, кіберзлочини вже набули транснаціонального характеру, і міжнародна спільнота, усвідомлюючи можливі негативні наслідки цього явища, намагається зменшити їх вплив на міжнародні економічні відносини» [203, с. 140].

Рада Європи відзначила транснаціональний характер комп'ютерних кримінальних правопорушень під час конференції з економічних злочинів у 1976 році. Основні риси транснаціональності вказані у статті 3, пункті 2 Конвенції 2000 року, в якій зазначено: «злочин має транснаціональний характер, якщо:

а) він відбувається в більш ніж одній державі;

б) він відбувається в одній державі, але значна частина його підготовки, планування, керівництва або контролю здійснюється в іншій державі;

в) він відбувається в одній державі, але за участю організованої злочинної групи, що діє в більш ніж одній державі; або

г) він відбувається в одній державі, але має значні наслідки в іншій державі».

Серед численних регіональних правових інструментів виділяється Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу, яка була прийнята 29 травня 2000 року [164], у частині судових доручень про перехоплення телекомунікаційних повідомлень (Розділ III «Перехоплення телекомунікацій»). Базовим документом у протидії кіберзлочинності для європейських держав, і не тільки, являється Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. та Додатковий протокол до неї від 28 січня 2003 р. Вони є «фундаментом для розробки відповідного законодавства європейських держав» [203, с. 140].

Висновки до Розділу 2

1. На цей час можна виділити основні напрямки еволюції злочинності у сфері інформаційних технологій в Україні: значний приріст кількісних показників; вагомий фінансовий стимул для більшості вчинених комп'ютерних кримінальних правопорушень; посилення методів та нові форми вчинення кримінальних правопорушень у сфері інформаційних технологій; підвищений професіоналізм осіб, що вчиняють кримінальні правопорушення у сфері інформаційних технологій; «помолодшання» комп'ютерних злочинців та збільшення кількості осіб, які раніше не притягали до кримінальної відповідальності; значні матеріальні збитки від кримінальних правопорушень у сфері інформаційних технологій у загальному обсязі збитків від інших видів кримінально протиправних діянь; зміна акценту в способах вчинення кримінальних правопорушень на використання комп'ютерних мереж; перехід злочинності у сфері інформаційних технологій до категорії транснаціональної; високий рівень латентності кримінальних правопорушень у сфері інформаційних технологій.

2. Різноманітні порушення в сфері інформації настільки розмаїті, що науковцями, національними правовими системами та міжнародним правом наразі ще не сформульовано загальної концепції цих порушень. Також відсутня єдність у термінології та система визнаних юридичних термінів, які б повністю відобразили всю різноманітність незаконних дій і наслідків у сфері інформації, інформаційних технологій, комп'ютерів та їхніх систем, локальних і глобальних інформаційно-телекомунікаційних мереж та інше.

Точно з цієї причини сучасні правові концепції потребують дальшого розвитку у напрямку розуміння сутності, основних характеристик, юридичних причин виникнення, наслідків порушень у сфері інформації, а також їхнього місця у загальній системі незаконної поведінки як на галузевому, так і на загальноправовому рівні, включаючи «міжнародні інформаційні злочини».

3. Кримінальні правопорушення, пов'язані з інформаційними технологіями, характеризуються підвищеною суспільною небезпекою, оскільки вони впливають на інші сфери, такі як власність, національна та громадська безпека тощо. Питома вага цих кримінальних порушень у відсотках є значно вищою, ніж 10 років тому. Отже, однією з найактуальніших проблем сучасності є

розробка оновленої стратегії запобігання злочинності у сфері інформаційних технологій, оскільки ця сфера дуже швидко змінюється, а злочинці постійно вдосконалюють методи вчинення кримінальних дій, що є невідомими правоохоронним органам.

4. У міжнародній правозастосовчій практиці питання кримінальної юрисдикції залежить від існуючого поділу кіберзлочинів за колом об'єктів: кримінальні діяння, спрямовані на конкретні об'єкти та завдають їм шкоду (наприклад, банківській установі, особистій електронній пошті тощо); кримінальні діяння, спрямовані на невизначене коло об'єктів та завдають їм шкоду (наприклад, поширення комп'ютерних вірусів, порнографічних матеріалів тощо).

РОЗДІЛ 3
ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

3.1. Сучасний стан запобігання злочинності у сфері інформаційних технологій

Розвиток комунікаційних мереж, інформаційних технологій та масової комп'ютеризації призвів до еволюції кримінально протиправних дій, що тепер охоплюють не тільки окремі держави, але й глобальне інтернет-співтовариство.

Суттєва частина кримінально протиправних діянь тепер відбувається в онлайн-середовищі. Інтернет надає злочинцям можливість вчиняти різні злочини, від шахрайства та крадіжок до більш серйозних діянь, таких як викрадення конфіденційної інформації, кібертероризм і кіберекстремізм. Це створює серйозні виклики для правоохоронних органів і суспільства в цілому.

Недостатня регуляція та соціальний контроль в онлайн-середовищі роблять інтернет ідеальним місцем для злочинців, які шукають анонімність та відсутність відповідальності. Тому важливо, щоб держави та міжнародні організації активно співпрацювали в розробці та впровадженні ефективних стратегій кібербезпеки та боротьби з кіберзлочинністю.

Ці стратегії можуть включати в себе законодавчі заходи, підвищення свідомості громадськості про ризики в інтернеті, розвиток технічних засобів кіберзахисту та міжнародну співпрацю для ідентифікації та припинення кіберзлочинців. Подолання цих викликів вимагає спільних зусиль на глобальному рівні.

Запобігання злочинності у сфері інформаційних технологій дійсно є актуальною та складною проблемою у сучасному світі. Зростання кількості та складності кримінальних правопорушень у сфері інформаційних технологій вимагає постійного оновлення та адаптації стратегій та заходів з кібербезпеки. Основні причини зростання цього виду злочинності включають в себе:

1. Технологічний прогрес: швидкий розвиток інформаційних технологій створює нові можливості для кіберзлочинців, такі як атаки на великі мережі та користувачів, використання розширених методів шифрування та анонімізації.

2. Анонімність в Інтернеті: інтернет надає злочинцям можливість діяти анонімно, що ускладнює їх ідентифікацію та затримання.

3. Глобальний характер кіберзлочинності: кіберзлочини можуть бути вчинені з будь-якої точки світу та спрямовані проти будь-якої іншої країни. Це ускладнює судове переслідування та співпрацю між державами.

Щодо ситуації в Україні, конфлікт з росією дійсно призвів до зростання кіберзлочинності, включаючи кібератаки та кібер-шпигунство. Цей конфлікт підкреслює важливість кібербезпеки для захисту національних інтересів та інфраструктури.

Так, від початку війни стало відомо про велику кількість кібератак на Україну.

Варто згадати невдалу спробу атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти конфіденційну інформацію.

Нещодавно Держспецзв'язку повідомило про отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання хакерами повного контролю над вашим комп'ютером та загрожує крадіжкою та пошкодженням комп'ютерних даних [316].

Раніше, 4 квітня, Держспецзв'язку попереджувало про розповсюдження електронних листів з назвою «Військові злочинці РФ.htm», відкриття яких призводить до того, що зловмисники отримують віддалений доступ до комп'ютера жертви [316].

«Під прицілом» знаходяться також об'єкти критичної інфраструктури. Український провайдер «Укртелеком» зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались проаналізувати, як влаштована IT-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії [149].

23 березня ворог намагався здійснити кібератаку на державні установи України з використанням шкідливої програми Cobalt Strike Beacon, яка уражає комп'ютер у випадку її відкриття [148].

Ми охарактеризували лише масовані атаки, які здійснювалися російськими хакерами на державні установи України. Про одиничні випадки офіційно не повідомляється, адже їхня кількість в кілька разів перевищує офіційну статистику. Саме тому необхідно

розглянути сучасний стан запобігання злочинності у сфері інформаційних технологій з метою пошуку оптимальних заходів її нейтралізації в умовах війни.

На сьогодні в Україні найпоширеніші види кримінальних правопорушень у сфері інформаційних технологій.

Фішинг: Кіберзлочинці створюють підроблені веб-сайти або відправляють шахрайські листи, які імітують легітимні організації або банки, з метою виманювання особистої інформації, такої як паролі та номери кредитних карт.

Мальваре (шкідливе програмне забезпечення): Це включає в себе віруси, черви, троянці та інші види програм, які можуть завдати шкоди комп'ютерам або використовувати їх для злочинних дій, таких як викрадення даних.

Скімінг: Злочинці встановлюють спеціальні пристрої, які копіюють дані з банкоматних карт під час транзакцій.

Кардинг: Злочинці використовують викрадені або підроблені кредитні карти для здійснення незаконних покупок.

Ддос-атаки (атаки з великою кількістю запитів): Злочинці завалюють веб-сервери або мережі запитами, щоб вимагати викуп.

Рейнджомерство (рансомваре): Злочинці захоплюють дані або блокують доступ до комп'ютера, вимагаючи викуп за їхнє повернення.

Протиправний контент: Це включає в себе розповсюдження порнографії, наркотиків, образливого контенту та інших матеріалів, що порушують закон.

Піратство: Незаконне копіювання та поширення програмного забезпечення, музики, фільмів та інших об'єктів інтелектуальної власності.

Онлайн-шахрайство: Фальшиві інтернет-магазини, аукціони та інші види шахрайства в інтернеті.

Крадіжка криптовалюти: Злочинці крадуть криптовалюту шляхом взлому гаманців або інших методів.

Рефайлінг: Незаконна підміна телефонного трафіку з метою викрадення інформації.

Соціальна інженерія: Злочинці використовують маніпулювання людьми, щоб виманити від них конфіденційну інформацію.

Це лише декілька прикладів кіберзлочинів, і цей список не вичерпний. Кіберзлочинність постійно розвивається, і кіберзлочинці винаходять нові способи атак та обхід заходів безпеки. Захист від

кіберзлочинності вимагає уважності та актуалізованих знань про кібербезпеку.

Отже, різноманіття видів кримінальних правопорушень, що вчиняються у сфері інформаційних технологій, свідчить про їх значну поширеність в нашій країні і проникли майже у всі сфери суспільної діяльності. Тому слід проаналізувати особливості запобігання таких кримінально протиправних діянь.

Саме тому аналіз кримінальних характеристик злочинності у сфері інформаційних технологій є важливим аспектом у розумінні і боротьбі з цією проблемою. Це допомагає розкрити генезис і механізми розвитку злочинності у цій сфері, враховуючи різні аспекти, які можуть впливати на цей вид злочинності. Вчені виокремлюють кілька ключових аспектів для аналізу злочинності у сфері інформаційних технологій: кримінально-правові характеристики: це включає в себе законодавчу базу, яка визначає, які дії вважаються кіберзлочинами, і які санкції передбачені для злочинців. Аналіз структури і змін у законодавстві щодо злочинності у сфері інформаційних технологій допомагає зрозуміти, які види діяльності вважаються злочинними і які кримінальні відповідальності передбачені; кримінологічні характеристики: цей аспект включає в себе аналіз розповсюдженості, структури та типів кримінальних правопорушень у сфері інформаційних технологій. Дослідження профілю кіберзлочинців, їх мотивації та методи дії також важливі для розуміння цього виду злочинності. Кримінологічні характеристики допомагають ідентифікувати ризики і способи запобігання таким кримінальним правопорушенням; соціально-демографічні характеристики: вивчення соціальних і демографічних аспектів злочинності у сфері інформаційних технологій, таких як вік, стать, освіта, професія та географічна розподіленість злочинців, може допомогти у визначенні факторів, які можуть бути пов’язані з цим видом злочинності [181, с. 8–9]. Остання група ознак стосується характеристики злочинців і потерпілих.

Однак отримання точної статистики щодо кримінальних правопорушень у сфері використання комп’ютерних технологій може бути викликаною задачею через декілька причин, включаючи: низьку латентність: багато кіберзлочинів залишаються непоміченими або не виявляються протягом тривалого часу. Злочинці, які вчиняють ці дії, можуть бути висококваліфікованими і вмілими в ухиленні від виявлення. Внаслідок цього, багато таких злочинів не

зафіксовані; труднощі ідентифікації: ідентифікація кіберзлочинців і припинення їх діяльності може бути вкрай важливою задачею. Злочинці можуть використовувати анонімні мережі та інші технології для приховування своєї сліду; підвідомчість: деякі кіберзлочини можуть бути непідвідомчими або важкодоступними для слідчих органів через міжнародний аспект, зокрема, коли злочинці вчиняють дії з інших країн; слабку звітність: не всі потерпілі реєструють або повідомляють про кіберзлочини, особливо якщо вони не супроводжуються фізичними збитками [332, с.178].

Однак незважаючи на ці обмеження, дослідники, правоохоронні органи та міжнародні організації все більше працюють над збільшенням розуміння та статистичної інформації щодо кіберзлочинності. Використання новітніх технологій і методів аналізу даних може поліпшити здатність виявлення та відстеження кіберзлочинців.

Крім того, обмін інформацією та співпраця між країнами щодо кіберзлочинності може сприяти вирішенню цієї проблеми. Міжнародні зусилля можуть допомогти в покращанні звітності і виявленні кіберзлочинців, які вчиняють злочини в різних країнах.

Зростання залежності від інформатизації та розвитку інформаційних технологій дійсно призводить до збільшення кіберзлочинності, адже більше можливостей для зловмисників означає більше потенційних атак на інформаційну інфраструктуру, особисті дані та фінансові ресурси. Професійні кіберзлочинці використовують ці можливості для особистої вигоди. Такі процеси впливають не лише на Україну, але й на багато інших країн.

Дослідження Інституту комп'ютерної безпеки США вказує на зростання загального збитку від кіберзлочинності. Цей тривожний тренд став загрозою як для індивідів, так і для організацій та держав. Для боротьби з цією загрозою важливо розвивати не лише технічні засоби захисту, але і вдосконалювати правовий статус і міжнародну співпрацю в сфері кібербезпеки [303, с. 202]. Відповідно до статистичних даних ГУБОЗ Міністерства внутрішніх справ України, на вересень 2000 р. в Україні було порушено 18 кримінальних справ, матеріальний збиток лише по одній з них становить 249 млн грн [351].

Зростання кількості кримінальних правопорушень у сфері інформаційних технологій в Україні свідчить про серйозну проблему злочинності в країні. Зокрема, статистика офісу Генерального прокурора свідчить про зростання цієї кількості цих кримінальних

правопорушень протягом останніх років. Такі кібернетичні атаки можуть мати серйозні наслідки для індивідів, організацій та держави.

Зокрема, з огляду статистичних даних Офісу Генерального прокурора випливає, що станом на 31 грудня 2022 року обліковано у звітному періоді 3 415 кримінальних правопорушень у сфері інформаційних технологій, що на 105 кримінальних правопорушень більше порівняно з 2021 роком та на 917 – більше порівняно з 2020 роком. Це свідчить в цілому про суттєве зростання, а саме – на 3,1 % порівняно з 2021 роком та – на 26,8 % порівняно з 2020 роком, кількості зареєстрованих кримінальних правопорушень [240].

Не зменшується кількість кримінальних правопорушень і в період воєнного стану. Зокрема це стосується кібершахрайства у фінансовому секторі. Так, упродовж дії воєнного стану слідчими Національної поліції України всього розпочато 789 кримінальних проваджень за фактами незаконних дій, пов'язаних з гуманітарною допомогою, благодійними пожертвами та безоплатною допомогою з такою правовою кваліфікацією:

– стаття 201-2 КК України – 630 (найбільше м. Києвом – 87, Львівською – 55, Дніпропетровською – 41, Хмельницькою – 34, Кіровоградською – 30, Харківською – 27 областями);

– стаття 190 КК України – 60 (найбільше м. Києвом – 10, Запорізькою – 10, Полтавською – 8, Житомирською – 9, Тернопільською областями – 4);

– стаття 191 КК України – 34 (Запорізькою та Полтавською – по 7, Львівською – 4, Сумською областю та м. Києвом – по 3, Харківською, Чернівецькою, Черкаською областями – по 2, Київською, Миколаївською, Житомирською, Херсонською областю – по 1);

– за іншими статтями КК України – 65 (Дніпропетровською – 20, Львівською – 11, Полтавською – 7, Чернівецькою – 6, Сумською – 4, Запорізькою, Миколаївською – по 3, Хмельницькою, Чернігівською та Вінницькою – по 2, Дніпропетровською, Харківською, Рівненською, Сумською областями та м. Київ – по 1).

Про підозру повідомлено сто п'ятдесят одній особі у 169 кримінальних провадженнях (Дніпропетровською – 24, м. Києвом – 19, Чернівецькою – 15, Полтавською – 14, Запорізькою, Львівською та Житомирською – по 12, Івано-Франківською та Миколаївською – по 8, Волинською, Рівненською – 6, Закарпатською, Вінницькою – по 5, Харківською та Одеською – по 4, Черкаською – 3, Хмельницькою,

Кіровоградською, Тернопільською, Чернігівською та ГСУ – по 2, Київською та Сумською областями – по 1) [219].

Сама тому аналіз кримінологічних характеристик правопорушень, пов'язаних з використанням комп'ютерних технологій, є дуже важливим етапом в розумінні та боротьбі з цими кримінальними правопорушеннями. Він може допомогти удосконалити законодавство, розробити більш ефективні стратегії боротьби з кіберзлочинністю та розмежувати відповідальність за різні види кіберзлочинів.

Аналіз таких характеристик дозволить оцінити ризики, з якими стикаються суспільство і індивіди, внаслідок кіберзлочинів, і розробити стратегії запобігання і відповіді на ці загрози. Він також може сприяти формуванню свідомості щодо кібербезпеки серед громадян та організацій, що є важливим чинником для зменшення ризику стати жертвами кіберзлочину.

Правильний аналіз кримінологічних характеристик може слугувати основою для розробки нового інформаційного законодавства, яке краще відповідає сучасним викликам і загрозам, пов'язаним з інформатизацією. Такі дані також можуть бути корисними для судів, правоохоронних органів та інших інституцій, які відповідають за боротьбу з кіберзлочинністю.

Розділ XVI Кримінального кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» містить низку норм, які передбачають кримінальну відповідальність за вчинення кримінальних правопорушень у сфері використання комп'ютерних технологій. Спеціальні статті, такі як ст. 361 (Незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж), ст. 362 (Викрадення, присвоєння, вимагання комп'ютерної інформації чи заволодіння нею шляхом шахрайства чи зловживання службовим становищем) і ст. 363 (Порушення правил експлуатації автоматизованих електронно-обчислювальних систем) встановлюють кваліфікуючі ознаки різних кримінальних діянь, пов'язаних із комп'ютерною злочинністю.

Ці статті дозволяють правоохоронним органам та судам накладати відповідальність на тих, хто вчиняє кіберзлочини, і визначати ступінь їхньої тяжкості відповідно до вчинених дій. Це важливий крок у визнанні серйозності кіберзлочинності та

намаганні обмежити і контролювати її національним законодавством.

Застосування цих спеціальних норм при кваліфікації комп'ютерних кримінальних правопорушень виконує не тільки кримінально-правову функцію, але й здійснює низку криміногічних функцій, у тому числі – забезпечення об'єктивності кримінальної статистики, наукових досліджень, формування емпіричної бази для напрацювання методик виявлення та розкриття кримінальних правопорушень, їх профілактики тощо.

Ефективність боротьби з кримінальними правопорушеннями у сфері використання інформаційних технологій значною мірою визначається розумінням криміналістичної сутності цього виду кримінально протиправного посягання. Розглянемо такий приклад. Припустимо, що зловмисник проник у комп'ютерну мережу банку і, вдавшись до маніпуляцій, перевів певну суму грошей на певний рахунок, з якого її благополучно зняв один із його співучасників.

Це кримінальне правопорушення можна кваліфікувати насамперед за ст. 361 КК України «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». У даному випадку можна вважати, що відбулося незаконне втручання в роботу банківської автоматизованої системи та несанкціонована зміна комп'ютерної інформації, яка містить дані про рахунки клієнтів банку, тобто перекручення інформації, а це якраз і входить у диспозицію згаданої статті. Під незаконним втручанням у роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж слід розуміти будь-яку форму втручання з використанням програмних та технічних засобів, призначених для незаконного проникнення, що дозволяє маніпулювати інформацією [178].

Зловмисник не мав законного права доступу до такої інформації, займаючись, з метою отримання несанкціонованого доступу незаконним збиранням кодів, які використовуються банками для захисту інформації. Відповідно до ст.14 КК України, його дії можна кваліфікувати як готування до кримінального правопорушення та усунення перешкод, а також інше умисне створення умов для вчинення кримінального правопорушення. Таким чином, дійсно сталося незаконне втручання в роботу банківської комп'ютерної системи, яке на додаток до всього ще й супроводжувалося незаконними операціями з засобами доступу до банківських рахунків,

що вже саме по собі може розглядатися як склад кримінального правопорушення, що підпадає під дію ст. 200, 231 КК України.

В результаті дій зловмисника з рахунку власника зникли гроші, тобто сталося крадіжка – таємне викрадення чужого майна на користь винного чи іншої особи, що заподіяло збиток власнику цього майна (ст. 185 КК України). Це не викликає сумніву, однак проблема полягає в тому, як кваліфікувати таку крадіжку. Кримінальний кодекс України говорить, що крадіжка може бути вчинена шляхом проникнення в житло, інше приміщення чи сховище. В нашому випадку можна стверджувати, що мало місце проникнення до сховища (розглядаючи банківську автоматизовану систему як сховище власності особи, якій заподіяна шкода), але мова не може йти про грабіж, розбій чи вимагання [178].

Обов'язковою ознакою крадіжки є таємне викрадення чужого майна. Це ж бачимо і в розглянутому випадку. Однак, при крадіжці передбачається, що відсутній обман як спосіб заволодіння чужим майном. Але тут обман очевидний, бо в результаті були переведені чужі гроші. Та власне гроші як матеріальний предмет украдені не були – було лише змінено відповідні реквізити в електронних записах, що призвело до зміни прав на володіння і розпорядження цим майном (грошима).

Ці дії можна кваліфікувати за ст.190 «Шахрайство» КК України, тобто заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. В ситуації, коли особа добровільно вводить свої фінансові реквізити та відправляє гроші шахраям через фішинг або інші кібершахрайські методи, складно вживати ст. 190 «Шахрайство» Кримінального кодексу України. Спроби кваліфікувати це як шахрайство можуть виявитися складними через те, що власник майна (у цьому випадку грошей) надавав фінансові реквізити свідомо і відправив гроші на власний розсуд. Тут більше відповідає статтям, які стосуються кіберзлочинів та інформаційних кримінальних правопорушень, таким як порушення правил експлуатації автоматизованих систем, незаконний доступ до комп'ютерних систем або інші спеціалізовані статті, які покривають інтернет-шахрайство та кіберзлочини. Очевидно, що в розглянутому випадку гроші не були передані добровільно, тому навряд чи можна кваліфікувати подібне кримінальне правопорушення як шахрайство.

Визначимося, в який момент вчинення кримінального правопорушення відбувається обман. Пам'ять комп'ютера можна розглядати як місце, де в електронному вигляді зберігається інформація про кошти, яка дозволяє проводити операції з ними. При цьому, як правило, використовуються спеціальні програмно-апаратні засоби захисту від несанкціонованого доступу до цієї інформації.

Злочинець використовує обман тільки в момент проникнення в банківську комп'ютерну мережу, при цьому призначенням проникнення є доступ до цінностей (у цьому випадку фінансових коштів), які зберігаються на комп'ютері. За кваліфікацією ця дія може бути розглянута як крадіжка з проникненням у сховище, як передбачено ст. 185.3 Кримінального кодексу України.

Така кваліфікація відображає сутність вчинку, а саме, що злочинець використовує обман для незаконного доступу до фінансових коштів на комп'ютері. Варто також враховувати, що при вчиненні таких дій, зазвичай є порушенням захисних засобів і систем безпеки, що може бути окремим обвинуваченням або аггравацією в розгляді справи.

Треба ще зазначити, що крадіжка визнається закінченим кримінальним правопорушенням тільки з моменту фактичного вилучення майна й наявності у злочинця реальної можливості розпоряджатися ним на свій розсуд. У цьому випадку така можливість з'являється з моменту завершення транзакції.

Отже, це комплексне кримінальне правопорушення, яке включає в себе незаконне втручання в роботу електронно-обчислювальних систем, несанкціонований доступ до комп'ютерної інформації, модифікацію цієї інформації і крадіжку коштів з рахунку потерпілого. Цей вид кримінальних правопорушень найчастіше практикується в сфері кредитно-фінансових установ і банків, де дії можуть призвести до серйозних фінансових втрат та порушень безпеки.

Способи кіберзлочинності, пов'язані з фінансовими операціями, постійно розвиваються, і злочинці намагаються знайти нові способи проникнення та маніпуляції інформацією. Для боротьби з цією проблемою важливо, щоб фінансові установи та банки зміцнювали свої заходи забезпечення кібербезпеки та моніторили свої інформаційні системи для виявлення можливих загроз.

Відомі на сьогодні способи характеризуються значною різноманітністю і постійно розширюються за способом їх вчинення. Це зумовлено як складністю самих засобів комп'ютерної техніки, так і

постійним нарощуванням нових інформаційних операцій, багато з яких забезпечують рух фінансових цінностей та коштів.

Дані проведеного нами анкетування вказують на те, що кримінальні правопорушення у сфері інформаційних технологій часто здійснюються спочатку безпосередніми працівниками організації, такими як програмісти, інженери та оператори (52 % опитаних). Це може бути особливо проблематично, оскільки ці працівники мають розширений доступ до інформаційних ресурсів і знання про внутрішні системи.

Крім того, доступ до комп'ютерної інформації і системи може бути здійснений ззовні, і віддалені способи доступу включають в себе атаки через мережу (27 % опитаних). Це може охоплювати різні види кіберзлочинності, включаючи вторгнення у мережеві сервери, злому паролів та різноманітні види атак, спрямованих на викрадення інформації, поширення вірусів тощо.

Для боротьби з цими загрозами важливо вдосконалювати кіберзахист і приймати заходи для недопущення несанкціонованого доступу до інформаційних систем. Це включає в себе моніторинг і виявлення можливих атак, регулярне оновлення програмного забезпечення для захисту, навчання персоналу з питань кібербезпеки та впровадження строгих правил доступу і паролів для зменшення ризику злому.

Віддалені атаки на комп'ютерні системи та мережі представляють серйозну загрозу кібербезпеці. Ці атаки можуть бути здійснені шляхом використання різних методів і технік і часто мають руйнуючий вплив на цільову систему чи мережу. Вони можуть включати в себе вторгнення в системи через віддалені канали зв'язку, експлуатацію вразливостей програмного забезпечення, атаки на мережеві протоколи та багато інших технік.

За нашими даними, віддалені атаки складають значну частину комп'ютерних кримінальних правопорушень (27 % опитаних). Це важливо враховувати при розробці заходів кіберзахисту. Для захисту від таких атак важливо використовувати сучасні методи обрання та виявлення вторгнень, моніторинг мережі для виявлення незвичайної активності, встановлення ефективних правил брандмауера та вдосконалення системи безпеки та автентифікації.

Поширення шкідливих програм на технічних носіях, таких як компакт-диски, є одним із способів впровадження шкідливого програмного забезпечення в комп'ютерні системи і мережі. Цей

метод може бути особливо ефективним для злочинців, оскільки він може використовуватися для зараження комп'ютерів інших користувачів, які встановлюють або використовують ці носії (21 %). Назви подібних компакт-дисків не відрізняються різноманітністю: «Хакери-2002», «Шпигунські штучки», «Халявний Інернет», «Все для хакера» тощо. До складу таких дисків звичайно входять різні набори програм, призначених для «злому» комп'ютерних систем, а також шкідливі програми – програмні закладки та віруси.

Дані щодо місця вчинення кримінальних правопорушень у сфері використання комп'ютерних технологій можуть бути корисними для розуміння звичайних місць та обставин, в яких злочинці вчиняють подібні правопорушення. Ці дані можуть слугувати для розвитку більш ефективних стратегій та заходів з протидії комп'ютерній злочинності та забезпечення кібербезпеки.

За вказаними даними, 50 % випадків анкетування свідчать про те, що кримінальні правопорушення в сфері використання комп'ютерних технологій вчиняються на місці постійного знаходження ЕОМ. Це може включати в себе власні комп'ютери користувачів або сервери в офісах, дому, або інших місцях.

У багатьох випадках віддалений доступ дозволяє злочинцям здійснювати атаки на комп'ютерні системи та мережі з місця, яке може бути віддаленим від їх фактичного місцезнаходження. Це робить важкою ідентифікацію та слідування за кіберзлочинцями, оскільки їх IP-адреси можуть бути приховані або масковані. Важко встановити точний фізичний адрес атакуючого, коли він або вона використовує віддалений доступ через анонімні мережі або проксі-сервери. Так, результати дослідження показали, що в 19 % випадків віддалений доступ здійснювався з комп'ютерного обладнання, розміщеного в будинку злочинця. У 6 % випадків доступ здійснювався з ЕОМ, яке було розміщене за місцем його роботи. У 3 % випадків злочинець використовував технічні можливості різних комп'ютерних центрів та клубів.

Окрім цього, поширення комп'ютерних вірусів є серйозною загрозою для безпеки інформаційних систем. Вони можуть завдати значних збитків, викрадаючи чи пошкоджуючи конфіденційну інформацію, завдаючи шкоди програмному забезпеченню та заволодіваючи комп'ютерами та мережами. Особливо важливою проблемою є поширення черв'яків через мережу Інтернет та електронну пошту.

Основними цілями й мотивами вчинення кримінальних правопорушень у сфері використання інформаційних технологій виступають: корисливість (73 % респондентів), хуліганські дії (9 %), помста (7 %), комерційне чи промислове шпигунство (8 %).

Як ми відмічали вище, кримінальні правопорушення у сфері використання комп'ютерних технологій у 5 разів частіше здійснюються чоловіками. Більшість суб'єктів таких кримінальних правопорушень має вищу або незакінчену вищу технічну освіту (53,7 %), а також іншу вищу чи незакінчену вищу освіту (19,2 %). Серед них переважають особи віком від 30 до 45 років 46,5 %), а також від 16 до 30 років (37,8 %).

Розглядаючи характеристику особи злочинця, треба зазначити що особливу категорію осіб, які здійснюють кримінальні правопорушення у сфері використання інформаційних технологій, становлять «хакери».

Як ми уже відмічали, хакери є особами, які володіють значними навичками у сфері обчислювальної техніки і інформаційних технологій. Їхні дії можуть бути спрямовані на одержання доступу до комп'ютерної інформації для різних цілей, включаючи фінансову вигоду, завоювання авторитету в хакерських спільнотах, або просто задоволення своїх технічних навичок.

Важливо розрізняти між хакерами, які діють в межах закону, і кіберзлочинцями, які вчиняють кримінальні правопорушення. Легальна діяльність хакерів може включати в себе етичний хакінг, аудит безпеки, а також роботу над виявленням і усуненням вразливостей в інформаційних системах. Деякі хакерські групи співпрацюють з організаціями, щоб поліпшити їхню кібербезпеку.

Проте кіберзлочинці використовують свої технічні навички для незаконних цілей, включаючи крадіжку інформації, шахрайство, атаки на комп'ютерні системи тощо. Така діяльність є незаконною і підпадає під кримінальну відповідальність.

Комп'ютерні хулігани є іншими категоріями осіб, які вчиняють комп'ютерні кримінальні правопорушення. Вони можуть завдавати збитків інформаційним системам і мережам, а також завдали значних проблем в різних галузях, включаючи глобальні телекомунікаційні мережі і критичну інфраструктуру.

Комп'ютерні хулігани зазвичай проводять атаки на вебсайти та сервери електронної пошти, з метою порушення роботи цих сервісів

або розповсюдження повідомлень. Це може призвести до збоїв у роботі і великих витрат для організацій.

Вірусні писаки створюють і поширюють комп'ютерні віруси, які можуть пошкодити комп'ютерні системи і дані. Їхні дії можуть мати серйозні наслідки, і вони можуть викликати значні збитки. Наприклад, атака вірусом «CIH (Chernobyl)» призвела до знищення бази даних енергетичних потужностей АЕС, і тільки через щасливий випадок аварія була уникнута.

Подібні інциденти свідчать про необхідність забезпечення адекватної кібербезпеки та прийняття заходів для запобігання атакам комп'ютерних хуліганів та вірусних писаків. Запровадження заходів щодо захисту інформаційних систем та посилення свідомості щодо кібербезпеки є важливими завданнями в сучасному інформаційному суспільстві.

Кримінальні угруповання, що діють у сфері інформаційних технологій, представляють серйозну загрозу як для інформаційної безпеки, так і для фізичної безпеки людей. Існує багато способів, якими такі угруповання можуть вчинити кримінальні правопорушення, використовуючи комп'ютери та мережі.

Наприклад, в лютому 1999 року у США був зафіксований випадок, коли комп'ютер використовували для здійснення вбивства. Для фізичного знищення важливого свідка, який знаходився в госпіталі під охороною агентів ФБР, злочинці після двох невдалих спроб його ліквідації за допомогою зброї, найнявши хакерів, через Internet проникли в локальну мережу цього госпіталю і змінили режим роботи кардіостимулятора та апарата штучної вентиляції легень, у результаті чого пацієнт помер. Його смерть здавалась цілком природною, як наслідок несумісності життя з пораненням. І лише згодом, після аналізу провайдером логічних файлів щодо доступу в локальну мережу, дійшли висновку, що несанкціоновано було змінено режим роботи кардіостимулятора.

Вказаний випадок в США є страшним прикладом того, як хакери можуть використовувати технології для вбивства або спричинення фізичних збитків. Зміна режиму роботи медичного обладнання через віддалений доступ до мережі госпіталю свідчить про те, як важливо забезпечити захист і безпеку важливих систем та обладнання.

Кібертерористи. Терористичні організації використовують інформаційні технології та Інтернет з кримінальними і нелегальними метами. Такі терористичні угруповання, як Hizbollah, HAMAS, the

Abu Nidal organization і Bin Laden's al Qa'ida використовують комп'ютерні файли, електронну пошту та шифрування (криптографію й комп'ютерну стеганографію) для підтримки своєї протиправної діяльності. Проте вони не застосовують кіберзброю за основним призначенням, проте застосовують новітні технології задля своїх незаконних дій. Кібертероризм, під яким розуміється використання сучасних інформаційних технологій, насамперед мережі Internet, коли така зброя застосовується з метою пошкодження важливих державних інфраструктур (таких, як енергетична, транспортна, урядова), може у недалекому майбутньому стати реальною загрозою для національної безпеки в першу чергу розвинутих країн світу.

Комерційне та промислове шпигунство в кіберпросторі представляють серйозні загрози для бізнесу та національної безпеки. Ось деякі важливі аспекти цих видів кіберзлочинів:

Викрадання інтелектуальної власності: комерційні суб'єкти та держави можуть використовувати кіберзасоби для викрадання конфіденційних бізнес-інформації, нових технологічних розробок, патентів та інтелектуальної власності у комерційних цілях.

Конкурентний шпигунство: компанії можуть наймати кібершпигунів, щоб отримати конфіденційну інформацію про своїх конкурентів, такі як бізнес-плани, цінову політику та маркетингові стратегії.

Державне шпигунство: держави можуть використовувати кіберзасоби для здобуття важливої конфіденційної інформації, включаючи військову та політичну інформацію, для підтримки своїх національних інтересів.

Ризик для національної безпеки: промислове та комерційне шпигунство можуть мати серйозні наслідки для національної безпеки, зокрема через втрату конкурентних переваг та здобуття інформації, яка може бути використана проти країни.

Співпраця та реагування: країни та компанії повинні співпрацювати для виявлення, припинення та розслідування актів комерційного та промислового шпигунства. Також важливо розробляти і вдосконалювати кіберзахисні заходи для захисту конфіденційної інформації.

Мережне шахрайство стало одним з найпоширеніших видів кіберзлочинів. Інтернет дійсно надає зловмисникам ідеальну

платформу для вчинення кримінальних дій, оскільки він дозволяє залишатися анонімним та має величезну аудиторію користувачів.

Мережні шахраї можуть використовувати різні схеми обману, включаючи шахрайство з фінансами, ідентичністю, інтернет-шахрайство та інші. Деякі з них використовують соціальний інженерінг, фішинг, шкідливі програми, щоб введення людей в оману і втягування їх у кримінальні схеми.

Маючи певний досвід, будь-хто, знаходячись у власній квартирі або офісі, може знайти ефективний спосіб обману через Internet, а сама глобальна інформаційна мережа є благодатним середовищем для вчинення різного роду кримінальних правопорушень. Характерним прикладом може бути випадок, коли 7 квітня 1999 року відвідувачі сайту фінансових новин компанії «Yahoo.Inc» виявили сенсаційне повідомлення. Оголошення, передане електронною поштою у розділі «Buyout News», повідомляло, що телекомунікаційна компанія «PairGain» в м.Тьюстин (США) переходить у володіння однієї з ізраїльських компаній. Додавалося також, що подробиці угоди можна взнати на веб-сайті Bloomberg News Service. Ця новина поширилася з неймовірною швидкістю і акції компанії, що продавалася, підвищилися в ціні більше ніж на 30 %. Обсяг продаж зріс майже в 7 разів. Проблема була тільки в тому, що угода – це обман, і веб-сайт, на якому з'явилася ця інформація, теж був підробкою, а не Bloomberg's-вебсайтом. Коли істина виявилася, ціни на акції різко впали, що призвело до великих фінансових втрат багатьох вкладників, які купили акції по штучно завищених цінах.

Інтелектуальні пірати. Питання інтелектуальної власності і боротьби з інтелектуальним піратством є важливими для економіки та суспільства. Нелегальне використання та розповсюдження інтелектуальної власності може завдати серйозних збитків авторам, компаніям і суспільству в цілому. Це також може призвести до поширення низькоякісних продуктів, які не відповідають стандартам якості.

У боротьбі з інтелектуальним піратством важливо розвивати ефективну правову базу та сприяти її виконанню. Також важливо проводити освітню роботу щодо важливості захисту інтелектуальної власності та надавати інструменти для легального доступу до інтелектуальних творів.

У зв'язку з тим, що злочинність у сфері інформаційних технологій не обмежена кордонами, міжнародна співпраця та обмін

інформацією між країнами стає все важливішою для боротьби з цим явищем. Розвиток та посилення кібербезпеки також є ключовими аспектами в боротьбі з інтелектуальним піратством, оскільки багато зловмисників використовують інформаційні технології для незаконного доступу до інтелектуальних творів [99].

Окрім цього, потрібно говорити й про інший спектр кримінальних правопорушень, що вчиняються у сфері інформаційних технологій.

Так, зловживання інформаційними технологіями може призвести до серйозних загроз суспільній безпеці. Кіберсуїциди є однією з таких загроз. Це небажане явище, коли люди шукають підтримку або відповідь на свої проблеми в онлайн-середовищі, інколи змушені зіткнутися з підтримкою або впливом інших, які можуть сприяти їхнім самогубствам [180]. Останнім часом швидко розвивається тенденція зростання кількості кіберсуїцидів, що є видом кримінальних правопорушень проти життя і здоров'я. В даному випадку спостерігається аутоагресія, яка знаходить вихід через пошук в мережі однодумців та спільне здійснення суїцидальних дій. В цьому випадку провідним мотивом є прагнення позбавитись болю, що виникає в кризових ситуаціях і який суб'єктивно сприймається як нестерпний, або ж бажання шляхом смерті утекти від проблем, з якими індивід не здатен впоратись. Найбільшим і відомим сайтом для самогубців Wired називає alt.suicide.holiday, скорочено a.s.h., що можна перевести, як «прах». Учасники цієї групи називають себе Ешера (Ashers), а ЗМІ вважають цей ресурс винним як мінімум в трьох випадках суїциду. Кореспонденти журналу Wired, поговоривши з родичами загиблих, готові підтвердити ще сім смертей, пов'язаних з a.s.h., протягом січня 2003 року [91].

Першим зафіксованим фактом вбивства, здійсненим за допомогою мережі Інтернет, був випадок, що відбувся в лютому 1998 р. в США. Важко поранений свідок кримінального правопорушення був захований в закритому госпіталі на території військової бази, проте злочинці через Інтернет-мережу змінили режим роботи кардіостимулятора і апарату вентиляції легенів, що призвело до смерті свідка. Та складність виявлення дій комп'ютерного злочинця полягає в його можливості вчиняти кримінальні правопорушення в кіберпросторі, у якого не має державних кордонів, що багаторазово збільшують ступінь її суспільної небезпеки.

Окрім цього, слід сказати про міждержавні конфлікти, які перейшли в інформаційний простір.

Починаючи з кінця 2013 року, конфлікти, що виникали, передусім, між державами, установами та організаціями, чи окремими особами перейшли у кіберпростір. Уряди провідних країн світу використовують різного роду кібератаки з метою пошкодження чи навіть ліквідації конфіденційної інформації або стратегічних ресурсів конкурентів та супротивників. Розглянемо найбільш типові загрози та об'єкти, що підлягають під кібератаку:

1. Мобільне рекламне програмне забезпечення (так зване «mobile advertising software» або «madware»). Така загроза може не лише перешкодити самому процесові використання пристрою, але також і вказати зацікавленим особам, хакерам ідентифікаційні дані вашого мобільного пристрою, місцезнаходження та контактні дані особи тощо. Спеціальна програма типу «madware», що непомітно потрапляє на пристрій користувача, паралельно встановлює додаткові програми, про які користувач до цього не здогадувався, а це, в свою чергу, створює нові ярлики, призводить до закидання користувача різними спливаючими вікнами, або ж навіть змінює налаштування браузера і водночас збирає його особисті дані, хоча сам користувач про це може й не здогадуватись. Тільки за 2013 рік кількість програм, що містять найбільш агресивні типи «madware», зросла на 210 %. На сьогодні загрозливі програми надсилають платні SMS-повідомлення, а перераховані кошти дістаються хакерам та зловмисникам.

2. Комп'ютерне програмне забезпечення, заражене вірусом, а також кібернапад. Однією з таких загроз є «ransomware», або шантажуюче програмне забезпечення, яке шифрує файли користувача та вимагає викуп за їх розблокування. Ця загроза стала досить поширеною та призвела до значних втрат для багатьох користувачів та організацій.

Крім того, «кібербуллінг» або «кіберзнущання» стає дедалі більшим клопотом в інтернеті. Це включає в себе онлайн-знущання, залякування, образи, а також поширення особистої інформації або фейкових повідомлень з метою засмучування або залякування інших користувачів. Кібербуллінг може мати серйозні емоційні наслідки для жертв і може виникати в політичному контексті, а також в інших сферах життя.

3. Соціальні мережі. Фінансування соціальних мереж формує нову серію загроз. Адже користувачі Інтернету з кожним днем усе з більшою довірою ставляться до різного роду соціальних мереж (наприклад, Vkontakte, Odnoklassniki, Mail.Ru Agent, Skype, Viber, Instagram, Facebook, Twitter тощо), включаючи обмін своїми особистими даними й купівлю спеціальної мережевої чи ігрової валюти і так званих віртуальних подарунків іншим користувачам. Із зростанням рівня монетизації соціальні мережі надають своїм активним користувачам можливість надсилати один одному також справжні подарунки у вигляді матеріальних цінностей, а не лише нематеріального об'єкта, в соціальних мережах відбувається зростання грошового обігу, що дає хакерам нові можливості для формування загроз та здійснення атак.

4. Платіжні операції в системі он-лайн та інтернет-банкінг (скажімо, Privat24 в Україні, Pekao24 у Польщі), що може стати потенційним об'єктом крадіжки особистих даних і призводить до обману користувачів та провокує останніх повідомити такі дані неофіційним соцмережам. Так, фішингові атаки (атаки із використанням фішингу) можуть включати в себе надсилання фальшивих сповіщень або листів, що запитують особисту інформацію від користувачів. Ця атака спрямована на обман користувачів і отримання їхньої конфіденційної інформації, такої як паролі, номери кредитних карток, соціальні номери та інше.

Зазвичай фішери вдаються до соціальної інженерії, спрямованої на створення обманливих листів або веб-сторінок, які схожі на ті, які використовують відомі сервіси або організації. Користувачі, які необачні або недостатньо обізнані, можуть натиснути на посилання або ввести свої особисті дані на фальшивих сторінках.

5. Електронні гаманці «eWallet», що поступово перетворюються у специфічний об'єкт, який хакери пробують використовувати у своїх цілях. «eWallet» можуть бути вразливими, що потенційно веде до крадіжки особистої інформації. Так, з ростом популярності мобільних платежів і збільшенням кількості транзакцій, які проводяться через мобільні пристрої, інформація про платіжні дані користувачів стає цінним об'єктом для хакерів і зловмисників. Під час таких атак хакери можуть використовувати різні методи, включаючи перехоплення Wi-Fi сесій або створення шкідливих програм для перехоплення інформації.

6. Так звані «хмарні» носії інформації типу «Cloud» (наприклад, e-Dysk, iCloud, Google Drive тощо). Включення до конкретної корпоративної мережі незахищених пристроїв, які накопичують інформацію, а після цього вона осідає вже на інших «хмарних» носіях, а це в свою чергу різко підвищує ризик витоку інформації або потенційного захоплення особистих незахищених даних. У результаті, встановлення користувачами нових програм призводить до зараження всієї системи [169].

Так, швидка комп'ютеризація та поширення Інтернету принесли безліч переваг, але водночас і нові виклики в глобальному інформаційному середовищі. Важливо розуміти, що кіберпростір став не тільки ареною для комунікації та доступу до інформації, але й місцем для кіберзлочинів, кібершпигунства та інших агресивних дій. Наявність та доступність великої кількості інформації в мережі може бути використана як для покращення національної безпеки, так і для нападів на неї.

Україна, також як і багато інших країн, визначає кібербезпеку як один із пріоритетних аспектів національної безпеки. Заходи щодо зміцнення кіберзахисту, розробка антивірусного програмного забезпечення, створення кіберзахисних структур та співпраця з іншими країнами на цьому полі стають дедалі актуальнішими. Важливо і надалі розвивати і вдосконалювати методи кіберзахисту, залучати фахівців у галузі кібербезпеки, ізольовувати критичні інфраструктури від потенційних загроз, інвестувати в кібернавчання і збільшувати свідомість громадськості щодо кібернебезпеки.

Кібершпигунство є серйозною загрозою в сучасному світі, оскільки це може призвести до витоку чутливої інформації, включаючи політичні, економічні та військові секрети. Кібершпигуни, так само як і кіберзлочинці, можуть використовувати різні техніки та атаки для отримання доступу до чужої інформації. Подібно до прикладу, який ви згадали, атаки шпигунства можуть мати серйозні наслідки, особливо якщо вони спрямовані на критичні інфраструктури або конфіденційну інформацію.

Розкриття шпигунських програм, таких як «Snake», виявлення схожостей з іншими відомими кіберзброями, наприклад «Stuxnet», свідчить про складні та високоорганізовані операції кібершпигунів. Деякі країни та організації вкладають великі зусилля в кібершпигунство для досягнення своїх політичних, військових чи економічних цілей. Дана програма дає змогу повною мірою вести

контроль над програмним забезпеченням. У вересні 2013 року в Україні побільшало кібератак на засоби масової інформації (ЗМІ) – 4 кібератаки, тоді як протягом усього літа було зафіксовано лише 2 DDoS-атаки на сайти ЗМІ. Наступні дані подає щомісячний моніторинг Інституту масової інформації (ІМІ) «Барометр свободи слова»: три літніх місяці поспіль 2014 року ІМІ фіксує збільшення кількості випадків кіберзлочинів проти журналістів та ЗМІ (у липні – 4, в червні – 4, у травні – 6, в квітні – 1, у березні – 18, в лютому – 5, у січні – 13) [17].

Кібератака на конфіденційну інформацію, зокрема на адміністрацію України та американські науково-дослідні університети зі структури НАТО, є серйозною кіберзагрозою. Використання «розриву нульового дня» в операційних системах Windows, що є надзвичайно вразливими, дозволяє хакерам отримати доступ до чутливої інформації і баз даних, пов'язаних з національною безпекою та іншими стратегічно важливими структурами. Це система, що провокує розрив у всіх версіях операційних систем, підписаних ОС Windows, починаючи з Windows Vista й закінчуючи Windows 8.1. Операційна система, яка була позбавлена помилки «zero-day» є Windows XP. Використовуючи ці знання, хакерам вдалося отримати доступ до даних щодо стратегічно важливих інститутів у структурах НАТО. Виявляється, що об'єктами кібершпигунства також стали нормативні документи з питань адміністрації України, бази даних американських університетів і багатьох інших установ, відповідальних за координацію питань, пов'язаних з національною безпекою в країні. Цей приклад показує, наскільки серйозною може бути загроза кібершпигунства для держав та організацій. Шпигунські операції можуть відбуватися на міжнародному рівні, і їхні наслідки можуть бути значущими. Для боротьби з цими загрозами країни повинні розвивати і зміцнювати свої кіберзахисні зусилля, а також співпрацювати міжнародно з іншими країнами для виявлення та відстеження кіберзагроз.

Спеціалісти Національного інституту стратегічних досліджень при Президентові України правильно визначили три основні проблеми, пов'язані із складністю боротьби проти кримінальних правопорушень у кіберсфері:

1) відсутність сформованих визначень ключових понять і термінів: Відсутність чітких визначень термінів у сфері кібербезпеки може ускладнити розуміння і комунікацію між правоохоронними

органами, урядовими установами та іншими структурами. Важливо розробити загальноприйняті визначення цих термінів для однозначного розуміння і співпраці.

2) нереформованість чинного нормативно-правового поля: брак адаптованих до сучасних кіберзагроз нормативних актів може перешкоджати ефективному реагуванню на кібератаки. Потрібна реформа законодавства, яка враховуватиме нові технології і методи кіберзлочинців.

3) відсутність Єдиної загальнодержавної системи протидії кіберзлочинності: важливо створити систему, яка об'єднуватиме зусилля правоохоронних органів, урядових інституцій та інших структур для ефективної боротьби з кіберзагрозами. Нормативне регулювання має забезпечити цю систему необхідними повноваженнями і ресурсами для ефективного функціонування [150].

Українським службам безпеки необхідно постійно моніторити діяльність та специфіку кіберзлочинів у віртуальному середовищі. Події 2013–2014 рр. на світовому рівні вказали на необхідність підсилення інформаційної безпеки [345].

Отже, ми підтримуємо думки науковців у тому, що швидкий та постійний науково-технічний прогрес створює нові можливості для кіберзлочинців, і, на жаль, кіберзагрози стають все більшими і складнішими. Збитки від кіберзлочинності дійсно можуть бути значно більшими, ніж від традиційних видів кримінальних правопорушень, і це створює серйозні загрози для компаній, урядових установ, індивідуальних користувачів та суспільства в цілому [301].

Наші висновки щодо запобігання кіберзлочинності відображають сутність комплексного підходу до цієї проблеми. Міжнародне співробітництво, правові заходи, технічні рішення та організаційні заходи є всіма необхідними компонентами для ефективного контролю та запобігання злочинності у сфері інформаційних технологій.

Міжнародний підхід: кіберзлочинність не зупиняється на кордонах держав, і міжнародне співробітництво важливо для обміну інформацією, ресурсами та координації дій для запобігання та розслідування кримінальних правопорушень у сфері інформаційних технологій.

Правовий підхід: удосконалення національних та міжнародних правових механізмів допоможе встановити відповідальність за кримінальні правопорушення у сфері інформаційних технологій і

впровадити ефективний механізм розслідування та судового переслідування злочинців.

Технічний підхід: забезпечення безпеки в інформаційному просторі вимагає використання сучасних технічних засобів та заходів, включаючи розробку і впровадження систем кіберзахисту, антивірусного програмного забезпечення, мережевих фільтрів тощо.

Організаційний підхід: групи, які займаються кіберзахистом, мають активно співпрацювати для розробки та впровадження профілактичних заходів, реагування на кіберзагрози та навчання громадськості щодо кібербезпеки [140, с. 177.].

Окрім цього, запобігання кіберзлочинності має включати в себе заходи віктимологічної профілактики – підвищення рівня цифрової грамотності населення і сприяння в просуванні індивідуальних засобів захисту особистої інформації. Актуальними є поглиблені виктимологічні кримінологічні дослідження кіберзлочинності, спрямовані на виявлення об'єктивних закономірностей, детермінант кіберзлочинності, характеристик окремих типів особистості кіберзлочинців, а також різних аспектів забезпечення кібер-безпеки [175, с. 212].

Кіберзлочинність справді є складним явищем, яке виявляється в низці різновидів діяльності, і вона може мати серйозні наслідки як для окремих осіб, так і для суспільства в цілому, та характеризується такими особливостями:

1) пов'язаність з іншими видами злочинності: це важлива істина, і важливо пам'ятати, що кіберзлочинці можуть використовувати технології для полегшення інших видів злочинності, таких як крадіжки, шахрайство, торгівля наркотиками і т. д. Ця взаємодія може робити їхню діяльність більш сильною.

2) високотехнологічний характер: так, це одна з головних рис кіберзлочинності, і вона вимагає від правоохоронних органів і підрозділів кібербезпеки великих зусиль, щоб боротися з цією загрозою.

3) латентність і виклики щодо виявлення: кіберзлочинність часто може залишатися невиявленою, оскільки вона може приховуватися в глобальному інтернет-просторі. Виявлення і розслідування кіберзлочинів вимагає великої експертизи та спеціалізованих ресурсів.

3) професійний характер і організованість: багато кіберзлочинців дійсно мають великий досвід та спеціалізацію в інформаційних

технологіях. Це робить їх важкими супротивниками для правоохоронців. Крім того, організована злочинність у цій галузі може виявлятися як великі міжнародні кіберзлочинні групи.

4) транскордонність і транснаціональність: кіберпростір дійсно існує поза кордонами, і це робить боротьбу з кіберзлочинністю значно складнішою. Міжнародне співробітництво є ключовим для ефективного реагування на цю загрозу.

5) динамічний розвиток інформаційних технологій: швидкі зміни в інформаційних технологіях створюють нові можливості для кіберзлочинців, а також вимагають постійного оновлення стратегій та методів для боротьби з цією загрозою.

6) економічний аспект: багато кіберзлочинів спрямовані на здобуття прибутку. Це може включати в себе крадіжки фінансових даних, інтернет-шахрайство та інші види фінансової махінації. Ось чому ця проблема часто класифікується як економічна злочинність.

7) політичний аспект: злочинці в кіберпросторі можуть також використовувати свої навички для політичних цілей. Це може включати в себе DDoS-атаки на урядові веб-сайти, кібершпіонаж, а також хакерські атаки, які проводяться на замовлення з метою впливу на політичну ситуацію. Важливо бути готовим до таких можливих загроз і розробити заходи безпеки для їх запобігання [171, с. 356].

Важливо бути підготовленими до викликів, пов’язаних з кіберзагрозами, і розглядати кібербезпеку як пріоритетну сферу національної безпеки. Саме тому можемо виокремити перспективи захисту кіберпростору в Україні:

1) Законодавство та стратегії: прийняття Закону про кібернетичну безпеку та розробка національної стратегії кібербезпеки є ключовими кроками. Ці документи нададуть важливий законодавчий та стратегічний каркас для боротьби з кіберзагрозами.

2) Охорона інтелектуальної власності: захист інтелектуальної власності є критично важливим в контексті кібербезпеки, оскільки багато атак спрямовані на витіснення конфіденційної інформації та інтелектуальних активів. Важливо розвивати засоби захисту цінної інформації.

3) Навчання і підготовка: внесення змін до навчальних програм та навчальних планів, що стосуються кібербезпеки, є ключовим для підготовки нового покоління фахівців у цій галузі. Забезпечення підготовки фахівців у галузі кібербезпеки допоможе розвивати кадровий потенціал країни.

4) Міжнародна співпраця: кіберзагрози часто транснаціональні, і співпраця на міжнародному рівні є ключем до їхнього вирішення. Україна може брати активну участь у міжнародних ініціативах та навчаннях з кібербезпеки, що сприятиме обміну досвідом та спільній боротьбі з кіберзагрозами.

5) Свідомість і готовність громадськості: важливо підвищувати свідомість громадськості щодо кібербезпеки і пропагувати культуру безпеки в інтернеті. Це може включати в себе навчальні програми для громадян і важливість звітування про кіберзагрози.

3.2. Нормативно-правове забезпечення запобігання злочинності у сфері інформаційних технологій

Збільшення кількості організованих груп і злочинних організацій, які використовують новітні інформаційні технології для здійснення кримінально протиправних дій, свідчить про те, що ця проблема стає все більш актуальною та складною для контролю.

Мережа Darknet дійсно створює анонімну платформу для злочинців і ускладнює розслідування та контроль з боку правоохоронних органів. Проте багато країн та міжнародних організацій спрямовують зусилля на боротьбу з цими викликами в сфері кібербезпеки. Важливо підкреслити, що правоохоронні органи національного та міжнародного рівнів співпрацюють для виявлення та припинення діяльності цих організацій. Так, за даними, наданими Національної поліції України, кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням новітніх інформаційних технологій, за останній рік збільшилась на 36 % [84].

Основною проблемою у сфері кібербезпеки є відсутність міждержавних кордонів у кіберпросторі. Це ускладнює виявлення, розслідування та припинення кіберзлочинів, оскільки зловмисники можуть діяти з будь-якої точки світу та завдають збитків в інших країнах.

Саме тому необхідно досліджувати і внутрішньонаціональне законодавство, і міжнародно-правове регулювання запобігання злочинності у сфері інформаційних технологій.

Дослідженням нормативно-правових питань запобігання злочинності у сфері інформаційних технологій займалися такі

вітчизняні науковці, як Н. М. Ахтирська, П. Д. Біленчук, В. М. Бутузов, В. Д. Гавловський, М. А. О. Г. Колб, Погорецький, В. Г. Хахановський, В. П. Шеломенцев, О. М. Юрченко та інші. Проте стрімкий розвиток інформаційних технологій та способів і методів протиправної діяльності у кіберпросторі спонукає для подальших досліджень.

Міжнародна спільнота дійсно визнає необхідність впровадження міжнародних механізмів та координації для запобігання загрозам у комп'ютерних мережах і кіберзлочинності. У травні 2011 року Міжнародний союз електрозв'язку і Управління ООН з наркотиків та злочинності підписали угоду про боротьбу з кіберзлочинністю [318]. Для прийняття конкретних заходів, спрямованих на обмеження комп'ютерних загроз ООН розробила Глобальну програму кібербезпеки, яка визначає п'ять основних напрямків для боротьби з цими загрозами:

1) законодавство і юридичні механізми: створення та вдосконалення національного та міжнародного законодавства для протидії кіберзлочинності. Це включає в себе визначення правопорушень, визначення відповідальності, видання запитів на видавництво кіберзлочинців, та інші юридичні аспекти.

2) технічні заходи і захист: забезпечення технічних заходів та створення інфраструктури для захисту інформаційних систем від кіберзагроз. Це може включати в себе застосування шифрування, виявлення загроз, запобігання інцидентам, та реагування на них.

3) співпраця та обмін інформацією: підтримка міжнародної співпраці між країнами та організаціями для обміну інформацією про кіберзагрози та інциденти.

4) інституційні та капацитетні розв'язки: розробка і зміцнення інституційних та капацитетних механізмів на національному та міжнародному рівнях для боротьби з кіберзлочинністю.

5) співпраця між секторами: співпраця між державними, приватними та громадськими секторами з метою спільної боротьби з кіберзагрозами.

На сьогодні можна виділити такі групи міжнародних і регіональних нормативно-правових актів, які регулюють суспільні відносини у сфері протидії кіберзлочинності:

1) Рада Європи: Європейська конвенція про кіберзлочинність (принята 2001 року) та додаткові протоколи, такі як Протокол про інкримінування діяльності національних груп, які спрямовані на

злочинну діяльність, яка здійснюється за допомогою комп'ютерних систем, та Протокол про інкримінування різних форм расистської та ксенофобної діяльності, використовуючи інтернет.

2) Європейський союз: Європейська стратегія кібербезпеки (прийнята в 2013 році) та Директива ЄС про мережеву та інформаційну безпеку (NIS Directive).

3) Шанхайська організація співпраці (ШОС): Декларація ШОС про створення інформаційного простору без військових загроз.

4) Ліга арабських держав: Арабська конвенція про кіберзлочинність та інші документи, які визначають співпрацю арабських країн у боротьбі з кіберзлочинністю.

5) Організація Об'єднаних Націй (ООН): ООН грає ключову роль у створенні міжнародних норм та стандартів у сфері кібербезпеки та кіберзлочинності. Наприклад, Глобальна програма кібербезпеки, яку було згадано раніше, представляє собою значущий документ в цьому контексті.

Поряд з нормативно-правовим регулюванням цього питання, існують і інші теоретичні підходи щодо вирішення проблем кіберпростору. Так, науковець Джон Перрі Барлоу ще у 1996 році запропонував розробити та прийняти Женевську декларацію незалежності кіберпростору, яка б передбачала функціонування Міжнародного суду у зв'язку тим, що кіберпростір не належить до жодної країни і є інтернаціональним. Проте цей документ так і не був прийнятий [369].

Організація Північноатлантичного договору (НАТО) визнає кіберпростір як важливий компонент сучасної безпеки і надає велике значення кіберзахисту. Оскільки кіберзагрози стали більш складними і руйнівними, а кібератаки можуть бути складовою гібридної війни, НАТО та її союзники вживають рішучих заходів для забезпечення кібербезпеки.

Національні агентства з кібербезпеки країн-членів НАТО співпрацюють з агентствами інших країн і спеціалізованими організаціями для виявлення, аналізу та протидії кіберзагрозам. НАТО розробило та впроваджує стратегію кібербезпеки, яка передбачає вдосконалення оборонних здібностей у кіберпросторі та готовність реагувати на кібератаки [385].

У випадку кібератаки на країну-члена НАТО, Альянс може вважати її атакованою, і це може викликати колективну реакцію. НАТО також розробило програму інформаційного обміну та

співпраці з партнерами з метою обміну інформацією щодо кіберзагроз та кібератак.

Активну позицію щодо протидії кіберзагрозам займають і міжнародні організації, У січні 2013 року у структурі Європолу в Гаазі (Нідерланди) розпочав свою роботу Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre – EC3).

Ці міжнародні і національні ініціативи свідчать про зростаючий обсяг уваги, який приділяється кіберзахисту та протидії кіберзагрозам. Ось деякі ключові моменти стосовно цих організацій:

1) Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre – EC3): EC3, розташований в Гаазі, Нідерланди, був створений Європолом у січні 2013 року. Основними завданнями EC3 є стратегічний аналіз стану кіберзлочинності, розробка політики та законодавства у сфері кіберзахисту і навчання правоохоронців. EC3 фокусується на боротьбі з кіберзлочинами, які вчиняються організованими кримінально протиправними групами і завдають серйозної шкоди жертвам, таким як інтернет-шахраївство і онлайн-сексуальна експлуатація дітей.

2) Національний центр з кібербезпеки Великобританії (National Cyber Security Centre – NCSC): NCSC був створений у Великобританії відповідно до Національного плану з кібербезпеки та Національної стратегії кібербезпеки 2016–2021 років. Його лондонський офіс був відкритий у лютому 2017 року. NCSC відповідає за забезпечення кіберзахисту та координацію кіберзаходів у Великобританії. Він також розробляє стратегії і плани дій для забезпечення національної кібербезпеки.

Загалом серед основних міжнародних нормативно-правових документів щодо протидії кіберзлочинності, у тому числі організованої, слід виокремити такі:

– Конвенція Організації Об’єднаних Націй проти транснаціональної організованої злочинності (United Nations Convention against Transnational Organized Crime), підписана у м. Палермо 12 грудня 2000 року та ратифікована із застереженнями і заявами Законом України від 04.02.04 р. No 1433-IV [162];

– Європейська конвенція про взаємну допомогу у кримінальних справах (European Convention on Mutual Assistance in Criminal Matters), підписана у м. Страсбурзі 20 квітня 1959 року та ратифікована із заявами і застереженнями Законом України від 16.01.98 р. No 44/98-ВР [254];

– Конвенція про кіберзлочинність (Convention on Cybercrime), підписана 23 листопада 2001 року в м. Будапешті і ратифікована із застереженнями і заявами Законом України від 07.09.05 р. No 2824-IV [255].

Отже, на міжнародному рівні запобігання злочинності у сфері інформаційних технологій здійснюється на належному рівні: сформовані універсальні та регіональні механізми запобігання цьому небезпечному явищу. Поряд з тим, сучасний стан міжнародного співробітництва свідчить про наявність нових загроз, які значно впливають на стан запобігання злочинності у цій сфері. Тому необхідно враховувати такі загрози і адаптувати законодавство як на міжнародному рівні, так і внутрішньодержавне.

Окрім цього, багато розвинених країн активно працюють над розробкою та прийняттям нормативно-правових документів і стратегій в галузі кібербезпеки та запобігання кіберзлочинності. Це дозволяє їм зміцнювати захист інформаційної інфраструктури, забезпечувати безпеку громадян та підприємств у кіберпросторі. Важливою частиною цих стратегій є визначення загроз, розробка і впровадження технічних та організаційних заходів для боротьби з кіберзлочинністю, сприяння інноваціям у сфері кібербезпеки, та співпраця з іншими країнами та міжнародними організаціями.

Серед зазначених країн США відзначаються активністю у галузі кібербезпеки, маючи стратегію національної кібербезпеки, а також Національний центр кібербезпеки і Центр з попередження кіберзлочинності. Франція, Німеччина, Великобританія, Канада та Японія також розробляють та впроваджують комплексні стратегії з кібербезпеки та активно співпрацюють у цьому питанні на міжнародному рівні. Ця співпраця допомагає розвивати міжнародні стандарти та норми в сфері кібербезпеки і управління кіберзлочинністю.

Так, на сьогодні найбільш розвинену систему таких нормативно-правових актів мають США. Не дивлячись на те, що в цій країні були прийняті одні з найперших у світі законів в даній галузі і сьогодні функціонують такі закони, як: Закон «Про злочини, пов’язані з засобами доступу» (Fraud and related activity in connection with access devices) [397], Закон «Про злочини, пов’язані з комп’ютерами» (Fraud and related activity in connection with computers) [398], Закон «Про перехоплення електронних повідомлень та прослуховування переговорів» (Wire and Electronic Communications Interception and Interception of Oral Communications) [399] тощо.

Особливістю законодавства США щодо запобігання злочинності у сфері інформаційних технологій є те, що воно постійно вдосконалюється відповідео до виявлених нових загроз. Так, the USA Patriot Act був прийнятий відповідно до подій, які сталися після терористичних актів 11 вересня 2001 року з метою зміцнення національної безпеки і боротьби з тероризмом. Закон надав широкі повноваження Федеральному бюро розслідувань (ФБР) і іншим агентствам щодо спостереження і розслідування різних видів злочинності, включаючи кіберзлочини.

Проте деякі положення The USA Patriot Act стали предметом критики через можливість порушення громадянських свобод і прав людини. У результаті цієї критики та з прагненням збалансувати національну безпеку зі збереженням приватності і прав громадян деякі положення були відмінені або змінені. Зокрема, у 2015 році був прийнятий закон «USA Freedom Act», який вніс зміни до The USA Patriot Act. Цей закон зменшив деякі повноваження стосовно масового збору даних і зберігання інформації про дзвінки громадян.

Такі зміни в законодавстві відображають постійний діалог між потребами національної безпеки та захисту приватності громадян. Уряди повинні знаходити баланс між цими інтересами, а також реагувати на змінюючіся загрози та технологічні можливості [395].

Нещодавно були прийняті Закон «Поширення інформації про кібербезпеку» (Cybersecurity Information Sharing Act (CISA), 2015 [365] та «Система покращення кібербезпеки критичної інфраструктури» (Framework for Improving Critical Infrastructure Cybersecurity) 2016 [372].

Для ефективного реагування правоохоронних органів на повідомлення про кіберзлочини необхідна дієва правова база для проведення слідчих (розшукових) дій та оптимальний баланс між дотриманням недоторканності приватного життя і повноваженнями з проведення розслідувань, оперативний доступ та засоби отримання електронних доказів у постачальників послуг мережі Інтернет, а також забезпечення належного навчання та технічних можливостей співробітників. Саме тому створення спеціальних підрозділів і правова база для боротьби з кіберзлочинністю є критичними компонентами ефективної протидії кіберзагрозам. Ці заходи допомагають забезпечити безпеку в інтернеті, а також збалансувати права та свободи громадян і підтримувати закон і порядок в цифровому середовищі.

Так, у США активно відбувається процес створення та реформування спеціалізованих підрозділів, які спеціалізуються на кібербезпеці і кіберрозслідуваннях, важливо для ефективної протидії кіберзагрозам, серед яких:

1) Відділ комп'ютерної злочинності та інтелектуальної власності (CCIPS): Цей відділ є частиною Міністерства юстиції США і спеціалізується на розслідуванні комп'ютерних злочинів і порушень інтелектуальної власності. Він грає важливу роль у захисті прав інтелектуальної власності та протидії кіберзлочинам.

2) Національна об'єднана група кіберрозслідувань (National Cyber Investigative Joint Task Force): Ця група є частиною Федерального бюро розслідувань (ФБР) і спеціалізується на розслідуванні кібератак, терористичних операцій і втручань у комп'ютерні мережі з-за кордону. Вона координує роботу різних агентств і служб для виявлення та припинення кіберзлочинності.

3) Цільова група протидії електронним злочинам (Secret Service on Electronic Crimes Task Forces): Секретна служба США грає важливу роль у захисті фінансових систем від електронних злочинів і має спеціалізовані групи для розслідування таких злочинів.

4) U.S. Army Cyber Command: Ця структура збройних сил США спеціалізується на кібервоєнних операціях і забезпеченні кібербезпеки для військових систем. Вона відповідає за захист мереж і інфраструктури армії в кіберпросторі та за можливість ведення кібероперацій в разі потреби.

Створення та активізація кіберкомандувань і спеціалізованих підрозділів у країнах світу свідчать про зростаючу увагу до кіберзахисту та кібербезпеки в умовах зростаючих кіберзагроз. Ці органи грають ключову роль у захисті країни в кіберпросторі та розслідуванні кіберзлочинів. Деякі країни, які виокремилися в цій галузі, включають:

1) Південна Корея: У 2009 році Південна Корея оголосила про створення підрозділу кібервійськ, що спеціалізується на кіберзахисті та кіберопераціях.

2) Велика Британія: в цій країні було створено National High Tech Crime Unit (NHTCU) у 2001 році для розслідування злочинів у сфері інформаційних технологій. Пізніше цей підрозділ був об'єднаний з The Serious Organised Crime Agency (SOCA) і став частиною National Crime Agency (національного агентства протидії злочинності) під

назвою National Cyber Crime Unit. Цей підрозділ спеціалізується на кіберзахисті та розслідуванні кіберзлочинів.

Розвиток кіберзлочинності в Україні, як і в багатьох інших країнах, вимагає активного оновлення та адаптації законодавства до нових викликів та загроз, пов'язаних із швидким розвитком інформаційних технологій. Для ефективного протидії кіберзлочинності і забезпечення кібербезпеки важливо приймати відповідні законодавчі акти та змінювати їх з часом. Однак нормативне регулювання не встигає за розвитком технологій, що значною мірою сприяє розвитку й поширенню кіберзлочинності.

Так, на сьогодні правове підґрунтя інформаційної безпеки України створюють: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про національну безпеку України» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов'язковість яких надала Верховна Рада України.

У Законі України «Про основні засади забезпечення кібербезпеки України» кібербезпеку визначено як захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі. Водночас кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем, тоді як кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [251].

У зв'язку з зазначеним сьогодні в Україні разом з докорінними змінами у зовнішньому та внутрішньому безпековому середовищі,

появою нових викликів та загроз в умовах гібридної війни активно реформується сектор безпеки і оборони з урахуванням специфіки кіберпростору. Так, Указом Президента України від 14 вересня 2020 року № 392/2020 затверджено Стратегію національної безпеки України, якою визначені основні пріоритети забезпечення кібербезпеки в державі [303].

З метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави окремим документом розроблена і затверджена Указом Президента України від 14 травня 2021 року №447/2021 Стратегія кібербезпеки України [303].

Указом Президента України від 13 лютого 2017 року No 32/2017 затверджено Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», у якому визначені термінові та короткострокові завдання Кабінету Міністрів України, правоохоронним органам щодо захисту інформації в інформаційно-телекомунікаційних системах, та зокрема на об'єктах критичної інфраструктури [239].

Поряд з нормативно-правовим забезпеченням, заходи боротьби з кіберзлочинністю повинні також супроводжуватися середньостроковими і довгостроковими стратегічними концепціями, спрямованими на захист інформаційних ресурсів і притягнення розробників кримінально протиправних схем до відповідальності.

Важливими аспектами такого підходу є:

1) стратегічний кіберзахист: розвиток стратегічних цілей і політики кіберзахисту допомагає визначити пріоритети та напрямки для зміцнення кібербезпеки країни. Це може включати в себе розробку національних стратегій кіберзахисту і створення центральних органів для координації цих зусиль.

2) усвідомлення загроз: важливо постійно аналізувати нові кіберзагрози та визначати їхні наслідки для національної безпеки.

3) розвиток кадрів: навчання і розвиток кадрів у галузі кіберзахисту є ключовим аспектом. Потрібно створювати програми навчання та підготовки, які допоможуть забезпечити наявність кваліфікованих фахівців.

4) міжнародне співробітництво: боротьба з кіберзлочинністю вимагає співпраці з іншими країнами і міжнародними організаціями.

Укладання міжнародних договорів та обмін інформацією є важливими аспектами цієї співпраці.

5) профілактика та свідомість громадськості: важливо надавати інформацію громадськості та бізнесу щодо кіберзагроз і заходів для їх попередження.

6) кримінальна відповідальність: законодавство повинно передбачати кримінальну відповідальність для кіберзлочинців і забезпечувати їхнє притягнення до відповідальності.

Окрім нормативно-правового регулювання запобігання злочинності у сфері інформаційних технологій, з ростом гібридних загроз і кіберзагроз до інформаційної інфраструктури країни, розвиток сектора безпеки та оборони стає надзвичайно важливим.

Так, 5 жовтня 2015 року був утворений Департамент кіберполіції – структурний підрозділ Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних Інтернет-мереж і систем [259].

Указом Президента України від 7 червня 2016 року No 242/2016 сформований Національний координаційний центр кібербезпеки, робочий орган в Раді національної безпеки і оборони України, на який покладено координацію заходів суб'єктів забезпечення кібербезпеки [246].

Водночас залишаються поки що невирішеними низка актуальних завдань, що визначені Стратегією кібербезпеки.

Зокрема, мова йде про невизначеність на законодавчому рівні таких понять, як кіберпростір, кіберзлочин, кібератака, об'єкти критичної інфраструктури та ін., що призводить до певних проблем в практичній діяльності правоохоронних органів, прокуратури та судів.

Так, невизначеність понять та відсутність чіткого законодавчого визначення ключових термінів у сфері кіберзахисту дійсно можуть створювати проблеми в роботі правоохоронних органів, прокуратури та судів. Чітке та уніфіковане визначення таких понять є важливим кроком для ефективного боротьби з кіберзлочинністю. Саме тому необхідно здійснити такі кроки:

1) Розробка визначень: укладання законодавчих актів або стандартів, які визначають ключові терміни, такі як «кіберпростір»,

«кіберзлочин», «кібератака», і т.д., допоможе уникнути невизначеності та створить загальноприйняте розуміння цих понять.

2) узгодженість з міжнародними стандартами: важливо також враховувати міжнародні стандарти та визначення, оскільки багато кіберзагроз та кіберзлочинів мають глобальний характер.

3) законодавчі поправки: в разі потреби слід розглядати внесення законодавчих поправок для уточнення визначень та понять у сфері кіберзахисту.

4) навчання та підготовка: працівники правоохоронних органів, прокуратури та судів повинні проходити навчання та підготовку щодо кіберзахисту та цифрових доказів, щоб бути здатними ефективно вирішувати кіберпитання та розглядати кіберзлочини.

5) розвиток експертизи: важливо розвивати експертизу у сфері кібербезпеки та цифрових доказів, яка допоможе визначати кіберзлочини та доводити їх в судовому порядку. Варто зазначити, що 78 % опитаних нами респондентів підтримали вказані дії.

Також наразі особливого значення набуває повна імплементація Конвенції про кіберзлочинність у частині таких статей:

– Стаття 16 – Термінове збереження комп'ютерних даних, які зберігаються;

– Стаття 17 – Термінове збереження і часткове розкриття даних про рух інформації;

– Стаття 19 – Обшук і арешт комп'ютерних даних, які зберігаються;

– Стаття 20 – Збирання даних про рух інформації у реальному масштабі часу;

– Стаття 21 – Перехоплення даних змісту інформації.

Підтримаємо пропозицію М.В. Гуцалюка, що зазначені питання доцільно вирішити прийняттям Закону України «Про основні засади забезпечення кібербезпеки України», проєкт якого знаходиться на розгляді в Верховній Раді України [110].

Не можна оминати увагою й інформаційну війну, яка ведеться росією проти України. Розуміючи це, у перший місяць війни парламент оперативно оптимізував кримінальне та кримінальне процесуальне законодавство, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців. Зокрема, були прийняті такі закони:

1) Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні

комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 року [235].

2) Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 року.

В сучасних умовах повномасштабної війни росії проти України особливу зацікавленість викликає останній нормативний документ, який вносить зміни до Кримінального кодексу України щодо посилення відповідальності за кримінальні правопорушення у сфері інформаційних технологій.

Так, метою нового Закону є:

1) посилення спроможностей та оптимізація національної системи кібербезпеки для протидії кіберзагрозам: Ця мета спрямована на зміцнення і вдосконалення існуючих структур та процедур для ефективної реакції на кіберзагрози та захисту національної кібербезпеки.

2) впровадження дієвих кримінально-правових механізмів протидії кіберзлочинності: Ця мета передбачає створення чітких та ефективних законодавчих засобів для боротьби з кіберзлочинністю та притягнення кіберзлочинців до відповідальності.

3) забезпечення надійності та безпеки використання цифрових послуг: Ця мета орієнтована на забезпечення безпеки та надійності цифрових послуг, що включає в себе заходи для захисту інформації та даних користувачів в цифровому середовищі.

Закон 2149-IX має на меті зміцнити національну кібербезпеку та створити ефективну систему захисту від кіберзагроз та кіберзлочинності в Україні.

Окрім цього, відповідно до Закону України «Про електронні комунікації» й вимог іншого законодавства України у сфері кібербезпеки, термін «електронно-обчислювальні машини (комп’ютери), автоматизовані системи, комп’ютерні мережі чи мережі електрозв’язку» замінено на «інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі» [238]. Відтепер ці зміни також задекларовані в Кримінальному кодексі України.

Проте, з огляду на ці зміни, виникають питання щодо трансформації термінології та встановленні посиленої відповідальності за

інші види кримінальних правопорушень у сфері інформаційних технологій.

Водночас незрозуміло, чому термінологію змінено лише частково, адже без змін залишилися формулювання назви розділу та інших статей з нього ж, де юридичні склади інших правопорушень також охоплюються поняттям «кіберзлочини». Є й інші відкриті питання. Так, ук практиків виникає питання щодо залишення без змін санкції за збут або розповсюдження інформації з обмеженим доступом залишилися без змін (ч. 1 ст. 361-2 ККУ). Проте у науці стверджується той факт, що зміни в термінології та законодавстві щодо кіберзлочинів і кібербезпеки можуть бути складними і вимагати часу для налагодження і роз'яснення. Внесення змін до законодавства – це постійний процес, і вони можуть викликати питання і недорозуміння на різних етапах впровадження. Однак такі зміни часто внесені з метою адаптації законодавства до зростаючих загроз і нових реалій сучасного інформаційного середовища.

Щодо питання про посилення відповідальності за розповсюдження або збут шкідливих програм порівняно із санкціями за збут або розповсюдження інформації з обмеженим доступом, це може відображати різні рівні шкоди і загрози для суспільства. Розповсюдження шкідливих програм може створювати загрозу для безпеки інформаційних систем і даних, тоді як розповсюдження інформації з обмеженим доступом може мати інші наслідки.

Окрім цього, відбулися зміни в конструкції частини 1 статті 361 Кримінального кодексу України, які спрощують формальний склад і не вимагають настання конкретних наслідків, можуть бути важливими для боротьби з кіберзлочинами в сучасному інформаційному середовищі. Важливо враховувати, що в кіберпросторі деякі дії можуть бути шкідливими і небезпечними, навіть якщо їх наслідки ще не проявилися чи не збагнулися.

Спрощення в Кримінальному кодексі України може полегшити проведення розслідування і винесення вироку за такі дії. Важливо, щоб такі зміни були розумними і відповідали загальній меті боротьби з кіберзлочинністю, забезпеченню кібербезпеки та захисту інтересів суспільства. Вони також можуть бути реакцією на зростаючі загрози у цій галузі і виклики, які виникають внаслідок розвитку інформаційних технологій.

Розширення і розмежування кваліфікованих юридичних складів кримінального правопорушення в статті 361 Кримінального кодексу

України важливий крок для забезпечення ефективного запобігання злочинності у сфері інформаційних технологій та притягнення їх виконавців до належної відповідальності.

В новій редакції до попередніх складів додаються такі кваліфіковані:

Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ч. 3 ст. 361 ККУ, новий кваліфікований склад, проте в попередній редакції диспозиція належала до опису основного складу).

Дії, передбачені частиною першою або другою цієї статті, якщо вони (…) створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (ч. 4 ст. 361 ККУ).

Дії, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану (ч. 5 ст. 361 ККУ) [177].

На нашу думку, додавання нових кваліфікованих складів, які стосуються витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації, створення небезпеки тяжких технологічних аварій, екологічних катастроф, загибелі чи масового захворювання населення, дозволяє більш точно враховувати різні аспекти кіберзлочинності та їх наслідки.

Важливо враховувати, що встановлення відповідальності за вчинення кримінальних правопорушень у сфері інформаційних технологій у період воєнного стану є важливим, оскільки воєнний стан може створювати особливі умови для кіберзлочинності та загроз кібербезпеці країни.

Зазначена реформа дозволяє більш точно кваліфікувати дії винних осіб і належним чином притягати їх до відповідальності за різні види кіберзлочинів та їх наслідки. Проте, важливо, щоб ці зміни були чіткими та однозначними для того, щоб юридична спільнота та судові органи могли правильно і рівноправно застосовувати закон.

Посилення санкцій за кримінальні правопорушення в сфері інформаційних технологій є важливим кроком у боротьбі з цими видами протирпавних діянь. Заходи цього виду повинні вислати суворий сигнал тим, хто намагається вчиняти кіберзлочини, і відлякувати потенційних порушників від вчинення подібних дій.

Посилення санкцій, особливо на кваліфікованих складах, може бути додатковою мотивацією для уникнення кіберзлочинів та зменшення їх поширення. Таким чином, воно сприяє збільшенню рівня кібербезпеки та захисту інформаційних ресурсів країни.

Наводимо у таблиці основні зміни щодо кваліфікації кримінальних правопорушень у сфері інформаційних технологій.

Кваліфікація в редакції закону 2149-IX	**Санкція за попередньою редакцією**	**Санкція в редакції закону 2149-IX**
Несанкціоноване втручання (ч. 1 ст. 361 ККУ)	Відсутня	Штраф від 17 тис до 51 тис грн або обмеження волі на строк до 3 років
Ті самі дії, вчинені повторно або за попередньою змовою групою осіб (ч. 2 ст. 361 ККУ)	Позбавлення волі від 3 до 6 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років*	Штраф від 51 тис грн до 119 тис грн або обмеження волі строком від 2 до 5 років, або позбавлення волі на той самий строк
Дії, передбачені ч.ч. 1 або 2 ст. 361 ККУ, якщо вони призвели до витоку, втрати, блокування інформації (ч. 3 ст. 361 ККУ)	Штраф від 10,2 тис до 17 тис грн, або обмеження волі від 2 до 5 років, або позбавлення волі до 3років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 2 років або без такого	Штраф від 119 тис до 170 тис грн або позбавлення волі на строк від 3 до 8 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років або без такого
Дії, передбачені ч.ч. 1 або 2 ст. 361 ККУ, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (ч. 4 ст. 361 ККУ)	В частині заподіяння значної шкоди – позбавлення волі від 3 до 6 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років* В інших частинах – відсутня	Позбавлення волі від 8 до 12 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років або без такого

Закінчення таблиці

Дії, передбачені ч.ч. 3 або 4 ст. 361 ККУ, вчинені під час дії воєнного стану (ч. 5 ст. 361 ККУ)	Відсутня	Позбавлення волі на строк від 10 до 15 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років
Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ч. 1 ст. 361-1 ККУ)	Штраф від 34 тис грн до 68 тис грн або виправні роботи на строк до 2 років, або позбавлення волі на строк до 2 років	Штраф від 34 тис грн до 68 тис грн або виправні роботи на строк до 2 років, або позбавлення волі на строк до 3 років
*За умови, якщо вказані дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації		

Також Закон 2149-IX передбачає, що втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не вважатиметься несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж, текст якого Держспецзв'язку зараз активно напрацьовує [177].

Запровадження змін, які дозволяють тестування державних інформаційних систем на наявність вразливостей, є важливим кроком у напрямку підвищення кібербезпеки та захисту державних інформаційних ресурсів. Багато інших країн вже успішно використовують програми Bug Bounty для виявлення і усунення вразливостей у своїх системах.

Ця ініціатива дозволить залучити талановитих інформаційних безпекових фахівців та етичних хакерів до покращення кібербезпеки державних систем. Однак важливо встановити чіткі правила і процедури для проведення таких тестувань, щоб уникнути можливих зловживань або несанкціонованого вторгнення в системи.

Зміни в конструкції статті 361 КК України, що дозволяють визнати незаконне втручання як несанкціоноване, якщо воно відбувається відповідно до Порядку пошуку та виявлення потенційних вразливостей, також відповідають поточним потребам

у забезпеченні кібербезпеки. Разом із запровадженням змін у законодавстві це сприятиме підвищенню рівня захисту інформаційних систем та допоможе зменшити кіберзлочинність.

Варто визнати й певну неповноту закону в цій частині. Від початку війни в Україні активізувався неофіційний громадський рух кіберопору ворогові, так звана «КіберАрмія». Подібний громадський рух, що активно захищає інтереси країни в кіберпросторі під час конфлікту або війни, може відігравати значну роль у захисті національної кібербезпеки. Оскільки дії таких осіб спрямовані на захист країни та громадян від кіберзагроз, було б доцільно формалізувати їхню діяльність та звільнення від відповідальності на рівні законодавства.

Такі заходи можуть включати встановлення чітких правил та процедур для громадських дій у кіберпросторі, які спрямовані на захист країни від кіберзагроз. Це може включати в себе механізми реєстрації, співробітництва з правоохоронними органами та інші аспекти, які б дозволили громадській спільноті безпечно та ефективно боротися з кіберзагрозами.

Дії українських громадян, які добровільно приєднуються до цього руху з метою захисту країни, слід визнати та підтримати як важливий елемент національної безпеки. Відповідне законодавство може допомогти врегулювати цю діяльність та забезпечити їй правовий статус.

Введення нового законодавства, яке регулює кібербезпеку та запобігання злочинності у сфері інформаційних технологій під час війни, є важливим кроком для захисту національних інтересів та безпеки громадян України в умовах кіберагресії. Кіберзлочини можуть завдати значної шкоди країні, і введення суворих санкцій та посилення відповідальності за такі злочини є важливим заходом для стримання потенційних злочинців.

Особливо важливим є запровадження відповідальності за кіберзлочини, що вчинені в умовах війни, оскільки вони можуть завдати серйозної шкоди національним інтересам та безпеці України. Такі дії можуть слугувати агресорові та ворогам країни, і, отже, несення відповідальності за них відповідає суспільним і національним інтересам України.

Дійсно, вимоги щодо захисту кіберпростору та боротьби з кіберзлочинністю є особливо актуальними під час війни. Важливо вдосконалювати законодавство та забезпечувати ефективний захист

інформаційних ресурсів та систем, щоб запобігти можливим кібератакам та мінімізувати їхні наслідки для країни та громадян.

Збереження безпеки в кіберпросторі під час війни є обов'язком кожного громадянина і суб'єкта господарювання. Спільна робота та співпраця з правоохоронними органами, а також інформування про можливі кіберзагрози є ефективними способами захисту країни та громадян.

Важливо пам'ятати, що кожна дія в кіберпросторі має наслідки, і, незалежно від мети, важливо діяти відповідально та дотримуватися законів та норм, що регулюють кібербезпеку. Гармонізація зусиль громадян та суб'єктів господарювання з офіційними органами допоможе досягти максимальної ефективності в захисті країни в кіберпросторі під час воєнного стану [125].

Кіберзлочини стали важливою проблемою, яка вимагає негайних та результативних заходів. Держави в усьому світі, включаючи Україну, працюють над розробкою та впровадженням стратегій і програм запобігання кіберзлочинності, а також зміцнення інформаційної безпеки.

Загальна система запобігання злочинності у сфері інформаційних технологій має об'єднувати державні органи, правоохоронні структури, громадські організації та інші зацікавлені сторони. Вона також має включати в себе освіту та навчання населення, розробку сучасних технологій кіберзахисту, аналіз кіберзагроз та розробку ефективних стратегій відповіді.

Профілактика кіберзлочинів та підвищення рівня кібербезпеки вимагають поєднання зусиль усіх сторін – уряду, громадських організацій, бізнесу та громадян. Правильна інформаційна грамотність, своєчасне виявлення та відповідь на кіберзагрози, а також зміцнення інфраструктури та технологічних засобів для захисту даних та систем – все це грає ключову роль у забезпеченні кібербезпеки.

Завданням усіх сторін є розвинути цілісну стратегію протидії кіберзлочинності, спрямовану на попередження злочинності, виявлення та припинення кіберзагроз та зміцнення інфраструктури кібербезпеки. Разом з цим, поширення інформації та освіта в цій області є ключовими елементами успішної стратегії протидії кіберзлочинності [304].

Збільшення кількості кіберзлочинів в Україні та в інших країнах є глобальною проблемою й існують декілька загальних та спеціальних причин, які спричиняють це зростання:

1) висока завантаженість правоохоронних органів: завантаженість правоохоронних органів і неспроможність вичерпати всі кіберзлочини у відповідний спосіб можуть призвести до відсутності належного реагування на всі кримінальні правопорушення. Так, наприклад, у жовтні 2021 року було виявлено близько 299 160 кримінальних правопорушень [124].

2) анонімність та глобальний характер: кіберзлочинці можуть діяти анонімно та з будь-якої точки світу, що робить їх важко відстежуваними та призводить до складнощів у їх ідентифікації та затриманні.

3) технологічний прогрес: швидкий розвиток цифрових технологій створює нові можливості для кіберзлочинців і вимагає постійного оновлення методів захисту.

4) брак кібергігієни: відсутність належного кібернавчання та відповідальності серед користувачів може сприяти розповсюдженню кіберзагроз.

Окрім цього, участь громадськості має формальний характер. Хоча деякі нормативні акти й закріплюють певні повноваження громадян щодо запобігання злочинності, на практиці вони не мають жодної користі. Наприклад, Закон України «Про участь громадян в охороні громадського порядку і державного кордону» закріплюються права громадських формувань з охорони громадського порядку і державного кордону, проте реалізація цих прав у більшості випадках можлива лише за участі правоохоронних органів [260]. Щодо участі громадськості, важливо підвищити їхню свідомість щодо кіберзагроз і кібергігієни. Проєкти освіти та навчання щодо кібербезпеки можуть бути запущені на рівні держави та місцевого самоврядування. Залучення громадян до процесу виявлення та повідомлення про потенційні загрози може бути сприянням у боротьбі з кіберзлочинами.

Щодо спеціалістів і технічного оснащення, важливо забезпечити правоохоронні органи та спеціалістів сучасними засобами для виявлення, розслідування та запобігання кіберзлочинам. Також можуть бути створені спеціалізовані команди, які мають спеціалізуватися на кібербезпеці і взаємодіяти з громадськістю для ефективної боротьби з кіберзлочинністю.

Також відсутність значних успіхів у боротьбі зі злочинністю у сфері інформаційних технологій пояснюється низьким рівнем комп'ютерної грамотності населення через обмежений доступ до інтернет-комунікацій.

Так, за даними Міністерства цифрової трансформації, 4 мільйони українців живуть у населених пунктах, де немає жодного інтернет-провайдера. Ще 1,5 млн українців проживають на околицях населених пунктів, де провайдери є, але вартість підключення занадто дорога і часто перевищує кілька тисяч гривень. Всього понад 17 тисяч населених пунктів в Україні не мають інтернет-інфраструктури [275]. Недостатній рівень знань в галузі інформаційних технологій, робить значну частку населення нашої країни вразливими перед злочинцями, які використовують новітні інформаційні досягнення та кіберзлочинцями.

Отже, оскільки кіберзлочини перетинають кордони і зазвичай вчиняються через мережу Інтернет, вони потребують спільних зусиль держав і міжнародних організацій для ефективного запобігання та розслідування. Створення єдиного централізованого органу для боротьби з кіберзлочинами може сприяти більш координованому і ефективному реагуванню на кіберзагрози. Важливо, щоб цей орган мав необхідні ресурси, фахівців і технічне забезпечення для успішної роботи. Також, розробка і впровадження міжнародно-правових інструментів для боротьби з кіберзлочинністю є важливою складовою стратегії. Такі інструменти можуть визначити правила і процедури для співробітництва між країнами у справах, пов'язаних з кіберзлочинами, і визначити міру відповідальності за такі кримінальні правопорушення [285].

Варто також зазначити, що законодавча база України не містить спеціального акту, який би врегульовував питання запобігання злочинності у сфері інформаційних технологій. Так, Указом Президента України № 446/2021 на зміну про Стратегію кібербезпеки України 2016 року введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». В жовтні 2017 року Верховною радою України ухвалено Закон «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки,

повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [251]. У Кримінальному кодексі України кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку закріплено в розділі 16 [177]. Деякі норми щодо превенції містяться в Конституції України, в Кримінальному процесуальному кодексі України, проте вони є більш декларативними і потребують подальшого опрацювання та вдосконалення.

Саме тому, на основі вивчення офіційних статистичних даних правоохоронних органів України, наукових джерел з цієї тематики, повідомлень у засобах масової інформації, внесених змін до законодавства у зв'язку з повномасштабною інформаційною війною росії проти України та за результатами анкетування практичних працівників нами розроблено Проєкт Стратегії забезпечення інформаційної безпеки в Україні, в якій визначено: основні поняття та принципи забезпечення інформаційної безпеки; визначено перелік і повноваження державних органів у сфері захисту інформаційного простору від кібератак, а також перераховано загальносоціальні, спеціально-кримінологічні та індивідуально-профілактичні заходи запобігання злочинності у сфері інформаційних технологій, зокрема, в умовах воєнного стану.

3.3. Суб'єкти запобігання злочинності у сфері інформаційних технологій в Україні

Сучасне суспільство, яке використовує інформаційні технології, ґрунтується на повсякденному використанні кібернетичних засобів, таких як комп'ютери, телекомунікаційні мережі та інші гаджети для комунікації. Глобалізація та інтеграція інноваційних технологій, включаючи засоби комунікації та автоматизацію процесів у всіх сферах життєдіяльності, призвели до знищення кордонів та сплетіння національних економік та інфраструктур усіх країн світу.

Однією з ключових характеристик проблеми кіберзлочинності є її глобальний характер. Кібератаки можуть призупинити функціонування не лише приватних компаній, але і державних установ, і жодна країна повністю не захищена від таких загроз. Зараз дедалі більше уваги акцентується на тому, що потенційними джерелами кіберзагроз

можуть бути не лише окремі хакери або групи хакерів, але й держави, терористичні та злочинні організації тощо. Актуальність цього дослідження визначається тим, що структура злочинності останнім часом зазнає змін, не тільки в Україні, але й у всьому світі: традиційну транснаціональну злочинність, включаючи економічні комп'ютерні злочини, замінює більш складна та інтелектуальна кіберзлочинність.

Кілька проблем, пов'язаних із вивченням кіберзлочинності як явища та способів її запобігання, вже знайшли відображення в наукових працях вітчизняних і зарубіжних експертів, таких як Ю. Батурін, П. Біленчук, В. Бутузов, А. Волеводз, М. Вертузаєв, В. Пивоваров, Б. Романюк, В. Розовський, О. Ткачова, Т. Тропін, В. Цимбалюк та інших, які створили фундамент для наукового розуміння координації та співпраці у сфері запобігання кіберзлочинності та визначили основні ознаки цього явища, що дозволяє розвивати пріоритетні шляхи та напрямки боротьби з цією проблемою.

Ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» у 2017 році [250] (далі – Закон) стало необхідним кроком на шляху створення єдиної правової бази для боротьби з кіберзлочинністю. Однак визначення понять, таких як «кіберпростір», «кіберзлочин», «кіберзлочинність» і «кібербезпека», потребує особливої уваги. Неправильне формулювання цих понять може спричинити непорозуміння і ускладнити їх практичне використання. З урахуванням унікальних рис цього типу злочинності, законодавство про протидію та запобігання цим порушенням правових норм має бути розроблене з урахуванням міжнародних стандартів та наукових досягнень. Заходи для запобігання кіберзлочинності, які обмежуються національними кордонами, не будуть успішними без врахування досвіду інших країн та без міжнародного співробітництва. У сучасних умовах досягнення кібербезпеки для жодної навіть найрозвинутішої країни не є можливим без широкої міжнародної співпраці.

При обговоренні міжнародних питань щодо боротьби з кіберзлочинами важливо відзначити Конвенцію Ради Європи про кіберзлочинність, яка була підписана в Будапешті у 2001 році. Ця конвенція визнана серйозним кроком міжнародного співтовариства в напрямку запобігання кіберзлочинам. Незважаючи на те, що деякі недержавні організації, такі як «Фонд Електронних Меж» (Electronic Frontier Foundation, США), міжнародна організація «Суспільство Інтернет» (Internet Society), «Організація кіберправа і кіберсвободи» (Cyber –

Rights & CyberLiberties, Великобританія), «Кріптополіс» (Kriptopolis, Іспанія), висловлювали протести щодо підписання Конвенції. Вони стверджували, що Конвенція може загрожувати правам і свободам особи, розширювати поліцейські повноваження уряду і знижувати відповідальність держави в сфері правоохоронної діяльності, що також може порушувати принципи приватності.

Досягнення або удосконалення реалізації національних стратегічних підходів можливе лише через використання досвіду як урядових, так і недержавних організацій інших країн та залучення міжнародних інституцій. У сучасних умовах неможливо уявити собі державу, яка була б недостатньо захищеною і не займалася модифікацією своїх секторів зовнішньої безпеки для відповіді на сучасні виклики. Кіберзброя вже давно стала невід'ємною частиною будь-якої війни, будь то відкрита чи прихована. Владні структури провідних держав систематично розробляють нові заходи для протидії загрозам в кіберпросторі, а також удосконалюють методи забезпечення кібербезпеки.

Аналіз стратегій з кібернетичної безпеки Франції, Німеччини, Канади, Туреччини, Нідерландів і Австралії, проведений на основі тлумачень понять «кібербезпека» в зарубіжних стратегічних документах національного та міжнародного рівнів, вказує на значні відмінності у визначенні самої кібербезпеки. Ці відмінності визначають різницю у підходах, які застосовуються до формулювання відповідних стратегій і планів дій для забезпечення кібербезпеки [367, с. 67].

Дослідження проблем, пов'язаних із координацією дій спеціальних органів держав для запобігання кіберзлочинності та розробки сучасних механізмів боротьби з нею, є одним із пріоритетних напрямків для кожної держави. Зрозуміло, що кіберзлочинність має прямий вплив на глобалізацію інформаційних процесів та розвиток глобальних телекомунікаційних мереж.

Ефективна боротьба з кіберзлочинністю потребує не лише узгодження кримінального законодавства на міжнародному рівні, але і систематизації та адаптації процесуальних заходів для співпраці у сфері запобігання злочинності у сфері інформаційних технологій. На сьогодні не існує єдиної міжнародної системи для боротьби з кіберзлочинністю, яка б використовувалася всіма країнами світу. Для оцінки готовності інформаційних систем країн до кібератак був використаний рейтинг McAfee. Результати

показали, що тільки три країни, а саме Швеція, Ізраїль і Фінляндія, здобули найвищий бал 4,5 з 5, в той час як ще вісім країн, включаючи США, Великобританію, Францію та Німеччину, отримали другий результат 4 бали. Польща зайняла четверте місце з 3 балами. Деякі країни, зокрема Україна, не були включені до цього дослідження.

Слід звернути увагу на міжнародні організації, які займаються запобіганням кіберзлочинності, а також на країни з великою територією та населенням, оскільки ці чинники можуть впливати на готовність до кібератак.

Поняття суб'єктів запобігання злочинності у сфері інформаційних технологій виникає з поняття суб'єктів запобігання злочинності. Самим обґрунтованим визначенням суб'єктів запобігання злочинності є таке: це державні органи, громадські організації, соціальні групи, службові особи чи громадяни, які активно займаються розробленням і впровадженням заходів, спрямованих на передбачення, обмеження та ліквідацію криміногенних явищ та процесів, що породжують злочини, а також на їхнє недопущення на всіх стадіях злочинності. В цьому контексті, вони мають визначені права, обов'язки і несуть відповідальність за свої дії [92, с. 47].

Інформаційна безпека включає в себе такі компоненти: активності іноземних політичних, військових, економічних і розвідувальних організацій у сфері інформації; політику домінування окремих країн у глобальному інформаційному просторі; діяльність міжнародних терористичних груп; розробку концепцій інформаційних війн різними структурами; культурну експансію у відношенні до конкретних держав [196, с. 24].

Суб'єкти, які працюють над запобіганням злочинності у сфері інформаційних технологій, повинні формувати єдину та добре організовану систему як у функціональному, так і в організаційному аспекті. Але розмаїтість та складність кіберсуперництва, яке включає практично всіх ключових суб'єктів міжнародної політики, робить важким завданням знайти науково-методологічні підходи для пояснення цього явища та передбачення його майбутнього розвитку з метою надання корисних рекомендацій. Ми не прагнемо визначити конкретні інституції та системи для протидії кіберзлочинності, а лише намагаємося визначити загальний перелік існуючих суб'єктів, які працюють у цій галузі.

Завдання забезпечення кібербезпеки та засоби досягнення захисту інформації входять в обов'язки численних міжнародних організацій,

зокрема спеціалізованих агентств ООН, таких як ЮНЕСКО, МСЕ, Інтерпол і Європол, а також міждержавних організацій, таких як:

1. Азійсько-Тихоокеанське економічне співробітництво (The Asia-Pacific Economic Cooperation).

2. Група G7 (G7).

3. Організація економічного співробітництва та розвитку (Organisation for Economic Cooperation and Development, OECD).

4. Шанхайська організація співробітництва та інших.

Міжнародний союз електрозв'язку (ITU) намагається регулювати кібервідносини шляхом прийняття низки нормативних актів, які стосуються кіберпростору та визначають основні терміни, такі як «кібербезпека», «загрози кібербезпеці», «уразливості», а також надають систематизовані основні методи вчинення кримінальних правопорушень у сфері інформаційних технологій. Крім того, ці акти передбачають заходи для запобігання цього виду злочинності, такі як технічний захист та втручання в роботу мереж.

У 2008 році було засновано Спільний центр передового досвіду в галузі кібербезпеки НАТО (NATO Cooperative Cyber Defence Centre of Excellence, CCD CoE). Цей центр є атестованою міжнародною військовою організацією НАТО і призначений для розширення можливостей спільного кіберзахисту країн-членів НАТО, поліпшуючи співпрацю Альянсу у сфері кіберзахисту. Центр співпрацює з державним і недержавним секторами в галузі інформаційної безпеки.

Додатково Європол відіграє важливу роль у протидії кіберзлочинності. У січні 2013 року було офіційно відкрито Європейський Центр по боротьбі з кіберзлочинністю в Гаазі, Нідерланди. Цей центр спрямований на координацію та обмін інформацією між правоохоронними органами Європейського Союзу та третіми країнами, боротьбу з дитячою порнографією в Інтернеті, навчання кваліфікованих експертів з кіберзахисту, розробку методів для запобігання злочинності в галузі інформаційних технологій та захист стратегічно важливих ресурсів Європейського Союзу. Центр також планує співпрацювати з Глобальним інноваційним комплексом Інтерполу в Сінгапурі [7, с. 37].

У 2016 році Європарламент прийняв Директиву щодо безпеки мережевих і інформаційних систем (Директива NIS – DIRECTIVE (EU) 2016/1148). Дослідження, закріплене в Директиві NIS, передбачає, що для підвищення загального рівня кібербезпеки в ЄС потрібно забезпечити:

1. Відповідний рівень готовності держав-членів, вимагаючи від них створення команд інцидентів з комп'ютерної безпеки (CSIRT) та компетентного національного органу NIS.

2. Співпрацю між усіма державами-членами шляхом створення групи співпраці з метою надання підтримки і сприяння стратегічній співпраці та обміну інформацією між державами-членами.

3. Високий рівень безпеки в усіх секторах, які мають життєво важливе значення для економіки і суспільства, і, до того ж, значною мірою залежать від інформаційно-комунікаційних технологій.

Щодо окремих держав, вже в 1978 році в США у штатах Флорида і Аризона був прийнятий закон «Закон про кіберзлочини 1978 року» [364]. Цей закон не лише встановив першу форму кримінальної відповідальності за комп'ютерні кримінальні правопорушення, але також визначив початок нової ери – кіберзлочинів. Ця ера призвела до створення відповідних державних органів, які спрямовані на протидію кіберзлочинності.

Сполучені Штати Америки утворили систему органів для забезпечення кібербезпеки. Зокрема, важливим органом є Управління національної безпеки (Department of Homeland Security), в межах якого діє спеціальний кібербезпековий департамент, який виключно відповідає за безпеку високотехнологічних систем у США.

Крім того, існує Кіберкомандування (U.S. Cyber Command), яке керує спеціальними підрозділами з метою проведення розвідувальних операцій в мережах, захисту власних мереж, блокування та дезактивації структур супротивника, використовуючи можливості кіберпростору.

У Франції було створено низку державних і неурядових установ, які займаються запобіганням злочинності у сфері інформаційних технологій. Наприклад, Національна комісія з обчислювальної техніки та свобод (CNIL), яка спеціалізується на захисті персональних даних. У цифровому світі CNIL виступає регулятором персональних даних та підтримує фахівців в кіберпросторі у їхній діяльності, а також допомагає громадянам контролювати свої особисті дані та реалізовувати свої права. З 2004 року вона має повноваження накладати санкції на компанії, які порушують Закон про інформатику, файли та свободи від 1978 року [382].

Одним із аспектів запобігання злочинності у сфері інформаційних технологій є ініціативи такого органу, як Верховний орган поширення творів і охорони прав в Інтернеті (HADOPI). Цей орган покладає

зусилля для визначення та регулювання незаконного завантаження інформації. Другий варіант Закону про так звану «триступеневу заборону доступу до мережі Інтернет» був схвалений Вищим конституційним судом країни [382].

У межах правоохоронної системи Франції діють відповідні суб'єкти, які спеціалізуються на боротьбі зі злочинністю у сфері інформаційних технологій. Починаючи з 1998 року, Національна жандармерія визначила як пріоритетну діяльність розв'язання проблем, пов'язаних із інноваційними технологіями, і створила відповідні структури та навчальні заклади, включаючи:

1. Відділ кіберзлочинів технічного обслуговування судових досліджень та документації (STRJD), який відповідає за моніторинг Інтернет-мережі та виявлення кримінальних правопорушень проти людей і майна, пов'язаних із передачею нелегальних даних в Інтернеті.

2. Комп'ютерний і електронний відділ Інституту кримінального розслідування Національної жандармерії (IRCGN), який розробляє методи, засоби та програмне забезпечення для автоматичного виявлення педофілів та інших злочинців.

3. Відомчі бригади інформації та судових розслідувань (BDRIJ) та інші суб'єкти.

Додатковою ключовою організацією, що здійснює діяльність у сфері запобігання кіберзлочинності в Франції, є Національне агентство безпеки інформаційних систем (ANSSI). Це французьке агентство з кібербезпеки, яке співпрацює з державними спецслужбами. Основним завданням ANSSI є реалізація Французької національної стратегії цифрової безпеки, оголошеної в 2015 році. Ця стратегія визначає пріоритети діяльності ANSSI, включаючи захист і безпеку державних інформаційних систем, критично важливих інфраструктур, особистих даних та боротьбу із кібернасильством. ANSSI також сприяє підвищенню обізнаності та навчанню в цифровій безпеці, сприяє розвитку бізнесу цифрових технологій та забезпечує цифрову стратегічну автономію і стійкість кіберпростору.

Існує Організація з регулювання мережевих ігор та служба Tracfin, яка належить до Міністерства фінансів і спеціалізується на боротьбі з відмиванням грошей. Однак важливо зазначити, що ці організації також допомагають виявляти та розслідувати випадки відмивання грошей, які стали більш поширеними через використання Інтернету для цих цілей. Національна рада з цифрових технологій, яка

складається з представників приватного сектору, має значний вплив на розробку законодавства щодо Інтернету. Ці організації є незалежними від уряду та відіграють важливу роль у формуванні політики в галузі цифрових технологій.

Сучасні заходи щодо запобігання кіберзлочинності включають проведення спільних навчань. Під час цих навчань ідентифікуються недоліки і вразливості інфраструктури, розробляються сценарії можливих атак і інцидентів, та обговорюються найбільш ефективні способи реагування та координації.

Cyber Europe Training, наприклад, включає симуляцію значних кіберінцидентів, які ескалюються до рівня кібернетичних криз. Ці навчання надають можливість аналізувати передові технічні кібер-інциденти та розв'язувати складні ситуації щодо безперервності бізнесу та кризових ситуацій. Вправи Cyber Europe Training базуються на реальних сценаріях, розроблених європейськими кібербезпековими експертами [381].

Наприклад, Cyber Storm (США) [18]. Учасники Cyber Storm виконують наступні завдання:

– аналізують можливості організацій, що готуються, захищаються та реагують на потенційні кібератаки;

– приймають стратегічні рішення і забезпечують міжвідомчу координацію відповіді на інциденти відповідно до політики та процедур національного рівня;

– підтверджують механізми обміну інформацією та комунікації для збору та поширення інформації про кіберситуації, реагування та відновлення інформації про кіберінциденти.

Результати дослідження сприятимуть розумінню системи заходів і суб'єктів, що працюють на запобігання кіберзлочинності, і впливають на сучасне законодавство України, як імплементовані міжнародні норми.

Отже, жодна з класичних теорій та схем функціонування державних інституцій не може повністю відповісти на питання, як належить концептуалізувати наявні знання про кібербезпеку та роль основних суб'єктів міжнародних відносин у цій сфері. Злочинність у сфері інформаційних технологій представляє собою новий вимір людської діяльності, який відзначається глобальністю та від-сутністю обмежень державних кордонів. Вплив злочинності у сфері інформаційних технологій охоплює різні верстви населення і включає в себе специфічну систему внутрішнього контролю та

відповідь правоохоронних органів. Кілька чинників сприяє поширенню кіберзлочинності, включаючи процеси глобалізації світової економіки та розвиток інформаційних технологій, зокрема Інтернет-ресурсів.

Порівняльний аналіз досліджень передового зарубіжного досвіду в галузі боротьби з кіберзлочинністю свідчить, що цей вид злочинності має тенденцію до зростання. Однією з умов цього зростання є ускладнення сучасних телекомунікаційних та технічних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій для широкого кола користувачів через особисті комп'ютери.

Враховуючи вищезазначене, існує необхідність у взаємодії між правоохоронними та іншими органами різних держав з метою забезпечення стабільності кіберпростору та кібербезпеки. Потрібна діяльність спільних міжнародних підрозділів для розслідування кіберзлочинів та прийняття заходів щодо кібербезпеки, як національних, так і всесвітніх. Таким чином, вдосконалення чинного законодавства з врахуванням міжнародного досвіду допоможе не тільки визначити межі кіберзлочинності в Україні і правильно кваліфікувати дії осіб, які вчиняють кіберзлочини, але і запобігти їхньому вчиненню в майбутньому [304].

Державні органи та інші спеціалізовані організації виконують завдання запобігання злочинності у сфері інформаційних технологій шляхом впровадження відповідних заходів з попередження злочинності, які включають розробку системи дій у суспільстві з метою запобігання кримінальним правопорушенням (соціальним, економічним, правовим), а також координацію діяльності правоохоронних та громадських організацій у межах комплексних програм для протидії кіберзлочинності та інших відповідних заходів. Суб'єкти, що здійснюють запобігання кіберзлочинності, мають створювати інтегровану систему, яка б увійшла в їх функціональну та організаційну структуру [304]. Проте аналіз статистики кіберзлочинів в Україні свідчить про те, що дії, спрямовані на їх запобігання, не є належно ефективними. Серед численних аспектів, що перешкоджають досягненню мінімізації кількості можливих кіберзлочинів, можна виділити загальні та специфічні причини. До загальних аспектів можна віднести наступне: в першу чергу, обмежені можливості співробітників правоохоронних органів через високе робоче

навантаження. Наприклад, у жовтні 2021 року було зафіксовано приблизно 299 160 кримінальних порушень [124].

В даний момент спостерігається зростаюча тенденція до звернення громадян до правоохоронних і судових органів з метою відновлення своїх прав і вимоги компенсації за завдану шкоду [94]. Перш за все, працівники уповноважених органів мають велику завантаженість і практично не встигають реагувати на звичайні кримінальні правопорушення, не кажучи вже про кіберзлочинність.

По-друге, як ми уже зазначали, в Україні відсутній спеціальний правовий акт, що регулює питання запобігання злочинності. Наприклад, Указом Президента України № 446/2021 було внесено зміни до Стратегії кібербезпеки України 2016 року та введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року щодо Стратегії кібербезпеки України. Також, у жовтні 2017 року Верховною радою України було ухвалено Закон «Про основні засади забезпечення кібербезпеки України», який встановлює правові та організаційні засади для забезпечення захисту життєво важливих інтересів людини, громадянина, суспільства та держави в кіберпросторі. Цей Закон визначає основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері та основні принципи координації їхньої діяльності з питань забезпечення кібер-безпеки [250]. Кримінальні правопорушення, які стосуються використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, а також мереж електрозв'язку, містяться в розділі 16 Кримінального Кодексу України [177]. Деякі положення щодо превенції вміщені у Конституції України та Кримінальному процесуальному кодексі України, однак вони в основному мають декларативний характер і вимагають подальшого вдосконалення та конкретизації.

Також участь громадськості здебільшого обмежена формальними межами. Наприклад, Законом України «Про участь громадян в охороні громадського порядку та державного кордону» надаються права громадським формуванням щодо забезпечення громадського порядку та державного кордону, але на практиці реалізація цих прав переважно залежить від участі правоохоронних органів [260]. Крім того, важливість превентивної роботи щодо кримінальних правопо-рушень практично не сприймається суспільством. Держава не надає

жодного стимулу для активної участі громадян у запобіганні злочинності. Люди не виявляють інтересу до превенції кримінальних правопорушень, доки ці кримінальні правопорушення не порушують їхні права та інтереси. Поширення принципу «моя хата з краю» набуває все більшого поширення.

Щодо спеціальних причин, що стосуються саме запобігання злочинності у сфері інформаційних технологій, по-перше, технічне оснащення органів та фахівців не відповідає сучасному рівню. Під час вчинення протиправних дій кіберзлочинці використовують передові технології, тоді як попереджувальна та розслідувальна робота проводиться з використанням застарілих комп'ютерів та обладнання.

По-друге, оскільки кіберзлочинність зазвичай має міжнародний характер і вчиняється особами різних національностей і з територій різних держав, міжнародне співробітництво набуває важливого значення. Європейський Союз приймає низку актів, що регулюють боротьбу з кіберзлочинністю, такі як Директива про боротьбу із сексуальною експлуатацією дітей в Інтернеті та дитячою порнографією (2011 рік) і Пропозиція про тимчасове регулювання обробки персональних та інших даних з метою боротьби із сексуальним насильством над дітьми (2020 рік), серед інших. Крім того, Європол створив Європейський центр з кіберзлочинності для підтримки розслідувань у цій галузі. Незважаючи на те, що Україна ратифікувала численні міжнародні договори, що передбачають співробітництво у боротьбі з кіберзлочинністю, на практиці співпраця з іншими країнами супроводжується складними бюрократичними процедурами, що значно уповільнюють процес запобігання кіберзлочинам.

По-третє, неефективність боротьби з кіберзлочинністю може бути пояснена низьким рівнем комп'ютерної грамотності серед населення через обмежений доступ до Інтернет-комунікацій. За даними Міністерства цифрової трансформації, 4 мільйони українців проживають в населених пунктах, де жоден Інтернет-провайдер недоступний. Ще 1,5 мільйона громадян мешкають на околицях населених пунктів, де є провайдери, але вартість підключення часто надто висока і може перевищувати кілька тисяч гривень. Усього понад 17 тисяч населених пунктів в Україні не мають доступу до Інтернет-інфраструктури [275]. Недостатній рівень інформаційної грамотності значної частини населення нашої країни робить їх вразливими перед

злочинцями, які використовують останні досягнення в інформаційних технологіях та стають кіберзлочинцями.

Подальший прогрес науки, техніки та інформаційних технологій спричинив появу нового виду злочинності – кіберзлочинності, яка відрізняється високим ступенем новизни та мобільністю. Це означає, що традиційні методи боротьби зі злочинністю потребують суттєвого удосконалення. Оскільки кіберзлочинність має міжнародний та транскордонний характер, міжнародне співробітництво та розробка міжнародно-правових інструментів важливі для ефективної боротьби з нею. Перегляд національного законодавства відповідно до міжнародних стандартів також важливий [285].

Держава повинна приділяти більше уваги запобіганню кіберзлочинності через адекватне фінансування та технічне забезпечення відповідних органів. Крім того, може бути доцільним перегляд організаційної структури боротьби з кіберзлочинами, наприклад, створення єдиного централізованого органу, що підпорядковується виконавчій владі. Такий орган може відігравати ключову роль в запобіганні злочинності у сфері інформаційних технологій в Україні.

Кіберполіція (Департамент кіберполіції Національної поліції України) представляє собою міжрегіональний територіальний підрозділ Національної поліції України та є частиною кримінальної поліції. Відповідно до законодавства України, ця організація відповідає за виконання державної політики у сфері протидії кіберзлочинності та організацію і проведення оперативно-розшукової діяльності відповідно до чинного законодавства.

Основні функції кіберполіції включають:

1. Виконання державної політики у сфері протидії кіберзлочинності.
2. Інформування громадськості про нові випадки кіберзлочинів.
3. Розробка та впровадження програмного забезпечення для систематизації та аналізу інформації, пов’язаної з кіберінцидентами, кіберзагрозами та кіберзлочинами.
4. Реагування на запити від закордонних партнерів, що надходять через Національну цілодобову мережу контактних пунктів.
5. Організація навчань працівників поліції з використанням комп’ютерних технологій у боротьбі зі злочинністю.

6. Участь у міжнародних операціях та співпраця в режимі реального часу з мережею контактних пунктів у понад 90 країнах світу.

7. Здійснення дій для протидії кіберзлочинам.

Кіберполіція відіграє ключову роль у забезпеченні кібербезпеки та боротьбі з кіберзлочинністю в Україні.

Протидія кіберполіції кіберзлочинам у сфері використання платіжних систем включає в себе такі види злочинів:

– Скімінг (шимінг) – незаконне копіювання інформації з треків магнітних смуг або чипів банківських карток;

– Кеш-трапінг – викрадення готівки з банкоматів шляхом встановлення спеціальних утримуючих накладок на шатрах банкоматів;

– Кардінг – незаконні фінансові операції, які використовують платіжні картки або їх реквізити без згоди власників;

– Несанкціоноване списання коштів із банківських рахунків через системи дистанційного банківського обслуговування.

У сфері електронної комерції та господарської діяльності кіберзлочини включають:

– Фішинг – спроби виманювати логіни та паролі користувачів Інтернету для доступу до електронних гаманців, сервісів онлайн-аукціонів та інших фінансових операцій;

– Онлайн-шахрайство – незаконне заволодіння грошима громадян через Інтернет-аукціони, Інтернет-магазини, веб-сайти та телекомунікаційні засоби зв’язку.

У сфері інформаційної безпеки важливо боротися з такими видами злочинності:

– Соціальна інженерія – маніпулювання людьми в Інтернеті для отримання конфіденційної інформації;

– Віруси та шкідливе програмне забезпечення (malware) – створення та поширення шкідливих програм і вірусів;

– Розповсюдження контенту, що порушує закон – включає екстремізм, тероризм, порнографію, культ жорстокості та насильство;

– Рефайлінг – незаконна підміна телефонного трафіку.

У сфері інтелектуальної власності важливо боротися з наступними злочинами:

– Піратство – незаконне поширення інтелектуальної власності в мережі Інтернет;

– Кардшарінг – надання незаконного доступу до супутникового та кабельного телебачення.

Суб'єкти забезпечення кібербезпеки:

1. У справі забезпечення кібербезпеки, що є невід'ємною частиною національної безпеки України, координація дій реалізується Президентом України через Раду національної безпеки і оборони України, яку він очолює.

2. Національний центр кібербезпеки, який функціонує на рівні Ради національної безпеки і оборони України, відповідає за координацію та нагляд за діяльністю суб'єктів, які забезпечують кібербезпеку. Крім того, він подає Президентові України пропозиції стосовно розробки та удосконалення Стратегії кібербезпеки України.

3. Кабінет Міністрів України відповідає за створення та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод громадян, і національних інтересів країни у кіберпросторі, а також за протидію кіберзлочинності. Він організовує та забезпечує належними ресурсами функціонування національної системи кібербезпеки та визначає вимоги і засоби для функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (за винятком банківської системи України).

4. Суб'єкти, які здійснюють конкретні заходи для забезпечення кібербезпеки в межах своєї компетенції, включають:

1) Міністерства та інші центральні органи виконавчої влади;

2) Місцеві державні адміністрації;

3) Органи місцевого самоврядування;

4) Правоохоронні, розвідувальні та контррозвідувальні органи, агентства оперативно-розшукової діяльності;

5) Збройні Сили України та інші військові формування, створені відповідно до закону;

6) Національний банк України;

7) Підприємства, установи та організації, які входять до переліку об'єктів критичної інфраструктури;

8) Суб'єкти господарювання, громадяни України та громадські організації, інші особи, які здійснюють діяльність або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, електронними правочинами, електронними засобами зв'язку, інформаційною безпекою та кіберзахистом.

5. Суб’єкти, в межах своєї компетенції:

1) Приймають заходи для запобігання використанню кіберпростору для воєнних, розвідувально-підривних, терористичних та інших незаконних і злочинних цілей;

2) Виявляють та реагують на кіберінциденти та кібератаки, та вживають заходів для усунення їх наслідків;

3) Здійснюють інформаційний обмін щодо вже сталося та можливих кіберзагроз;

4) Розробляють та реалізовують запобіжні, організаційні, освітні та інші заходи в галузі кібербезпеки, кібероборони та кіберзахисту;

5) Забезпечують проведення аудиту інформаційної безпеки, включаючи аудит на об’єктах, які підпорядковані їм або входять до сфери їх управління;

6) Здійснюють інші заходи для забезпечення розвитку та безпеки кіберпростору.

3.4. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні

Сьогодні практично кожна особа використовує Інтернет-технології в своєму щоденному житті, державні структури і приватні підприємства впроваджують електронний обіг документів, банківські установи опираються на автоматизовані електронні системи, і навіть функціонування залізничного транспорту вимагає використання електронних комунікаційних засобів. Інтернет-комунікації значно полегшують повсякденне життя людини, покращують роботу державних органів, органів місцевого самоврядування, підприємств, установ і організацій.

Але в процесі науково-технічного розвитку та активного впровадження Інтернет-технологій у всі сфери суспільства, зростає рівень злочинності. Згідно з офіційною статистикою Офісу Генерального прокурора, протягом останніх восьми років кількість виявлених кіберзлочинів зросла майже в 8 разів [240]. Однак у статистиці не враховано використання інформаційних технологій як засобу вчинення звичайних кримінальних правопорушень, хоча велика частина таких випадків на сьогодні є досить поширеною. Все це підкреслює необхідність проведення досліджень, узагальнення та розробки нових стратегій для запобігання таким кримінальним порушенням.

Особливої актуальності це питання набуває в Україні в сучасних умовах, оскільки за умов введеного воєнного стану кіберзлочинці активно використовуються для взлому урядових серверів, розповсюдження дезінформації серед населення та створення фейкових профілів у соціальних мережах тощо. Кібершахрайство, під час якого злочинці, видаючись представниками різних служб і організацій, намагаються отримати банківські реквізити громадян для незаконного заволодіння їх коштами, стало розповсюдженим.

Таким чином, війна в інформаційному просторі завдає суспільству не менше збитків, ніж збройний конфлікт на полі бою. З урахуванням цього, в Україні розпочато процес вдосконалення чинного кримінального та кримінального процесуального законодавства з метою притягнення кіберзлочинців до відповідальності. Все це підкреслює важливість обраної теми і необхідність дослідження чинного законодавства, судово-слідчої практики і наукових джерел з цього питання.

Багато вчених займалися дослідженням питань, пов'язаних із боротьбою з кіберзлочинністю. До числа таких дослідників входять О. М. Бандурка, В. В. Василевич, В. В. Голіна, Б. М. Головкін, А. П. Закалюк, О. М. Литвинов, В. В. Марков, М. І. Сащенко, В. І. Трапезніков, В. О. Туляков, І. В. Жук, Я. В. Левківська і багато інших. Проте питання запобігання кіберзлочинності в умовах воєнного стану залишається темою, яка не отримала вдосталь наукового аналізу і дослідження.

Слід відзначити, що законодавча база України не містить окремого спеціального акта, який би регулював питання запобігання злочинності у сфері інформаційних технологій. Натомість в українському законодавстві існують кілька правових актів, які стосуються даної теми.

Один з основних правових документів, що регулює запобігання кіберзлочинності в сфері інформаційних технологій, це Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. Згідно з цим законом, кіберзлочин (комп'ютерний злочин) – це винне суспільно небезпечне діяння в кіберпросторі або за допомогою нього, яке передбачено у кримінальному законодавстві України (ККУ) або визнано злочином за міжнародними договорами України. Такі дії мають на меті розкрадання або руйнування інформації в інформаційних системах та мережах [251]. У період війни кіберзлочини можуть бути вчинені

з метою порушення стабільності у країні, викрадення важливої (конфіденційної) інформації, паралізування роботи державних установ та технологічних систем, а також завдання інших матеріальних збитків.

Ці питання деталізовані у Стратегії кібербезпеки України, яка була введена в дію Указом Президента України № 446/2021.

Друга важлива річ полягає в тому, що оскільки злочинність у сфері інформаційних технологій зазвичай має міжнародний характер і вчиняється особами різних національностей і з територій різних держав, міжнародне співробітництво набуває надзвичайного значення. Європейський Союз прийняв низку актів, які регулюють питання боротьби з кіберзлочинністю, включаючи Директиву про боротьбу з сексуальною експлуатацією дітей в Інтернеті та дитячою порнографією (2011 рік), Пропозицію про тимчасове регулювання обробки персональних та інших даних для боротьби з сексуальним насильством над дітьми (2020 рік) та інші. З метою об'єднання європейської експертизи в галузі кіберзлочинності та підтримки розслідувань кіберзлочинності в Європі був створений ключовий орган Європейського союзу – Європейський центр з кіберзлочинності. Незважаючи на те, що Україною було ратифіковано кілька міжнародних договорів, які передбачають співробітництво в боротьбі зі злочинністю у сфері інформаційних технологій, на практиці співробітництво з іншими країнами супроводжується значною кількістю бюрократичних процедур, які відчутно уповільнюють процес запобігання таким кримінальним правопорушенням [285, с. 18].

Після повноцінного вторгнення росії на територію України кількість кримінальних правопорушень у сфері інформаційних технологій стрімко зросла. Країна-агресор активно використовує інтернет-технології для дезінформації щодо свого вторгнення на територію України та пропаганди ворожих ідей тощо. Відтак, Верховна Рада України провела оптимізацію кримінального та кримінального процесуального законодавства, покращуючи підстави та процесуальні механізми для притягнення злочинців до кримінальної відповідальності.

Зокрема, були внесені зміни до відповідних законів, таких як «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та

протидії кібератакам» № 2137-IX від 15 березня 2022 року і «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24 березня 2022 року [233].

Спеціальні зміни в законодавство були спрямовані на посилення кримінальної відповідальності за злочини у сфері інформаційних технологій та розширення повноважень правоохоронних органів для виявлення таких порушень закону.

На практиці після впровадження відповідних правових змін відзначається покращення ефективності боротьби зі злочинністю у сфері інформаційних технологій, в основному завдяки посиленню відповідальності за наведені кримінальні порушення. Проте залишається невирішеним питання щодо вивчення соціальних, економічних, політичних, демографічних, організаційних і інших причин, що призводять до кібершахрайства. На сьогодні для розробки системи запобігання злочинності в галузі інформаційних технологій використовуються лише результати судово-слідчої практики.

Необхідність у посиленні кримінальної відповідальності за порушення у галузі інформаційних технологій була актуальною вже протягом тривалого періоду. Зміни до законодавства включають в себе розширення повноважень правоохоронних органів для розслідування кіберзлочинів, які передбачені статтями 361 і 361-1 Кримінального кодексу України. Заходи, спрямовані на посилення санкцій та додаткове криміналізування окремих дій, можуть обмежити можливість потенційних злочинців вчиняти нові кримінальні правопорушення.

Надзвичайно важливим, на нашу думку, є впровадження відповідальності за вищезазначені кримінальні правопорушення, вчинені під час воєнного стану. За такі протиправні дії повинні передбачатися суворі санкції, оскільки обставини в країні вимагають цього. Особа, яка завдає шкоди національним інтересам України у кіберпросторі і таким чином допомагає агресору в цій війні, повинна нести відповідальність, аналогічно воєнним злочинцям.

Важливо зазначити, що сфера використання Інтернет-технологій давно потребувала посиленого захисту. Вторгнення росії стимулювало удосконалення чинного законодавства та зміцнення гарантій безпеки в сучасному інформаційному середовищі.

Від початку війни стало відомо про велику кількість кібератак на Україну. Зокрема, сучасним видом кібершахрайства в Україні є пенсійні афери, які пов'язані із шахраями, що пропонують неправдиві фінансові можливості, обіцяють великі суми грошей та гарантовану підтримку від фондів. На платформі соціальних мереж, зокрема на Facebook, активізувалися шахраї, які використовують тему фінансових виплат для українців. Про це повідомляє Державна служба спеціального зв'язку та захисту: «Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA), яка діє при Держспецзв'язку, зафіксувала збільшення кількості шахраївських сторінок на платформі соціальних мереж Facebook. Зловмисники використовують тему фінансових компенсацій і фінансової підтримки від ООН, Європейського суду з прав людини, Товариства Червоного Хреста» тощо [302].

Зокрема, шахраї обіцяють компенсації, які, за їхніми словами, будуть здійснюватися «за рахунок конфіскованих активів рф» і посилаються на недійсні рішення різних органів влади України. Повідомляється, що в оголошеннях їм пропонується перейти за посиланням, яке веде на фішингову сторінку, на якій розташований так званий «Єдиний Компенсаційний Центр повернення невиплачених грошових сум». На цьому веб-сайті користувачам запропоновано отримати компенсацію при умові надання особистої інформації та внесення додаткових платежів. Як результат, дані з банківської картки користувача можуть бути скомпрометовані [302].

Слід відзначити, що в Україні існує багато таких кримінально протиправних схем, які сьогодні активно використовуються. Боротьба з цією формою злочинності ускладнена через використання Інтернет-ресурсів, що робить складним виявлення кіберзлочинців. Крім того, кібершахрайство має міжнародний характер, що додатково ускладнює виявлення і запобігання такої злочинності. Це лише один із багатьох видів кримінальних порушень у сфері інформаційних технологій [36].

Погоджуємось з думкою вчених про необхідність не лише посилення відповідальності за кіберзлочини, але й розробку різноманітних соціально-економічних, організаційно-управлінських та морально-психологічних заходів, спрямованих на запобігання чинникам, що сприяють вчиненню кіберзлочинів.

Це важливо для побудови ефективної системи запобігання злочинності в галузі інформаційних технологій. Враховуючи

різноманітність факторів, які спонукають до кіберзлочинності, важливо впроваджувати заходи, які спрямовані на запобігання цій проблемі на різних рівнях.

Наприклад:

1) Органи державної влади і приватні підприємства можуть підвищити рівень кібербезпеки, залучаючи технічних спеціалістів або спеціалізовані компанії. Вони здатні підняти стійкість до кіберзагроз за допомогою впровадження необхідних алгоритмів захисту та надавати професійну інструкцію співробітникам, які працюють з інформаційними системами та мережами;

2) Особи, які перебувають у зоні ризику кібернападів, повинні слідкувати за офіційними повідомленнями на веб-ресурсах Держспецзв'язку та CERT-UA, оскільки органи поширюють інформацію про можливі кіберзагрози і надають поради щодо їх запобігання;

3) Якщо особа стає жертвою кібератаки, важливо сповістити інших, на кого ця атака може вплинути – інших працівників, клієнтів, контрагентів, родичів або друзів;

4) У разі кібератаки важливо інформувати офіційних суб'єктів забезпечення кібербезпеки в Україні, такі як CERT-UA та кіберполіція. Це допомагає вжити негайних заходів щодо блокування і нейтралізації шкідливих веб-ресурсів, а також виявити та притягнути до відповідальності злочинців.

Згідно Конституції України наша держава є демократичною, соціальною та правовою. Власне, саме тому «…людина, її життя і здоров'я, честь і гідність, недоторканість є найвищою соціальною цінністю» [168]. Дане положення є одним із головних в Основному законі нашої держави.

Право на доступ до публічної інформації є невід'ємною частиною загального права особи на інформацію. Необхідно відрізняти це право від загального поняття права на інформацію, оскільки воно більше широке і включає різноманітні аспекти. Право на інформацію означає свободу слова, а також включає в себе право збирати, зберігати та розповсюджувати інформацію.

З іншого боку, право на доступ до публічної інформації визначається як можливість отримання інформації. У сучасному суспільстві нормативне забезпечення права на доступ до публічної інформації є ключовою передумовою для існування демократії в державі.

Наукові дослідження відзначають пріоритетність прав людини на вільний доступ до інформації, право на свободу слова та думки, а також можливість отримувати інформацію про діяльність вищих органів держави та органів місцевого самоврядування в межах демократичної держави. У цьому контексті роль засобів масової інформації виявляється важливою, оскільки вони сприяють взаємодії з органами державної влади та місцевого самоврядування та розповсюджують інформацію серед громадян.

Для зміцнення демократії та підтримки прав і свобод громадян необхідно покращувати і розвивати взаємодію між органами держави та засобами масової інформації, зокрема зміцнюючи ефективність цієї взаємодії. [380].

У своєму науковому дослідженні Бодунова О. М. розглядає причини зростання кількості високотехнологічних протиправних діянь, зокрема кримінальних порушень, пов'язаних із використанням сучасних інформаційних технологій. Серед основних факторів, що сприяли цьому зростанню, автор виділяє наступні:

1. Широке використання сучасних інформаційних систем та технологій у різних сферах суспільного життя.

2. Швидке поширення інформаційних технологій, де головним підґрунтям для їх використання є глобальна мережа Інтернет.

3. Доступ до Інтернету для великої кількості користувачів, що сприяє поширенню цих технологій.

У 2014 році, після вторгнення росії на територію України, виникла необхідність створення системи для забезпечення кібербезпеки країни. Це стало актуальним внаслідок воєнних дій та інформаційно-психологічного впливу, що супроводили вторгнення, а також через постійні кібератаки в інформаційному просторі України [49].

російські окупанти, починаючи з 24 лютого 2022 року, додатково до активних воєнних дій, нападів на мирне населення, знищення житлових будинків і розкрадання власності мешканців, проводять активну інформаційну кампанію. Ця кампанія включає в себе створення фіктивних профілів в соціальних мережах з метою знаходження інформації про розташування Збройних Сил України та територіальної оборони, а також дезінформацію мирного населення. Через мобільний зв'язок надавалася неправдива інформація українцям з метою змусити їх повертатися до зони активних бойових дій. Також було проведено активну інформаційну атаку на

загальнодержавні ЗМІ для зупинення поширення інформації про російську агресію та вбивство мирних громадян.

З цієї причини, найважливішою є співпраця представників державних структур і територіальної оборони з представниками медіапростору. Їх співпраця спрямована на виявлення, розкриття та запобігання майбутніх злочинів, таких як встановлення осіб, які стали жертвами кримінальних правопорушень, та їх свідків, отримання інформації про обставини протиправних дій, виявлення та затримання осіб, причетних до злочинів, відновлення викраденого майна та інших слідів злочинів.

Ми вважаємо, що взаємодія правоохоронних органів і ЗМІ повинна сприяти виявленню, розкриттю та запобіганню злочинів. Вона сприяє оптимізації ресурсів та поліпшенню результативності правоохоронної діяльності у важливих сферах, таких як розслідування злочинів, оперативні заходи, правопорядок і профілактика злочинності. Зміцнення такої співпраці важливо для розвитку демократії та підтримки прав та свобод громадян. [20].

Для правоохоронних органів корисним є використання медіапростору у своїй діяльності, оскільки це надає можливість зміцнити законність і правопорядок в країні. Ця діяльність спрямована на підвищення правової культури громадян та спонукає їх поважати законодавчі норми та роботу правоохоронних структур.

Згідно із статистикою, яка подана в звіті Офісу Генерального прокурора, протягом 2019 року представники прокуратури України звернулися до ЗМІ 60 089 разів, зокрема: 6 277 разів в друкованих виданнях, 9 962 рази в електронних ЗМІ, 10 023 рази до інформаційних агентств, 33 544 рази до Інтернет-джерел і 52 рази до акредитованих закордонних ЗМІ. Порівнявши ці дані з аналогічним періодом 2020 року, можна відзначити, що протягом перших трьох місяців цього року представники прокуратури України звернулися до ЗМІ 15 864 рази, включаючи 1 568 разів в друкованих виданнях, 2 163 рази в електронних ЗМІ, 3 018 разів до інформаційних агентств, 9 047 разів до Інтернет-джерел та 55 разів до акредитованих закордонних ЗМІ. Порівнявши ці дані, можна відзначити, що вони перевищують показники за аналогічний період попереднього року на 19 відсотків [133].

Щодо вище викладеного, слід відзначити, що в умовах воєнного стану взаємодія між правоохоронними структурами і представни-

ками ЗМІ потребує певних напрямків для подальшого удосконалення. Зокрема, це включає у себе необхідність поліпшення законодавчих норм, що чітко визначають взаємовідносини між сторонами. Додатково, важливо акцентувати увагу на оперативності поширення інформації про заходи, проведені правоохоронними органами, а також підвищити компетенцію представників ЗМІ.

Отже, питання щодо взаємодії між правоохоронними органами та ЗМІ у контексті запобігання злочинності під час воєнного стану потребує подальшого розвитку та удосконалення, що може бути реалізовано представниками наукової спільноти в галузі кримінального права та кримінології. Ця проблема стала актуальною для наукового пошуку.

Про російську пропаганду та її вплив на український медійний простір говорять вже вісім років. У грудні 2014 року в Україні було створено Міністерство інформаційної політики, однією з його функцій було протидіяння російській агресії. Крім того, у вересні 2019 року було створено Міністерство цифрової трансформації України, яке стало центральним виконавчим органом, відповідальним за реалізацію політики держави у сфері цифрової трансформації, відкритих даних, державної інформації, інтероперабельності мережевих систем, надання послуг через електронні пристрої та системи, а також підвищення рівня цифрової грамотності населення.

Погляди науковців і практиків розходяться щодо ролі журналістів у війні: деякі вбачають, що журналісти мають бути «воїнами» у цьому конфлікті, тоді як інші наполягають на тому, що ЗМІ повинні виконувати свою головну функцію – чесно інформувати громадськість.

Ця дискусія особливо важлива у формуванні взаємодії між ЗМІ та правоохоронними органами під час запобігання злочинності. У воєнний період це питання набуває актуальності як серед науковців, так і серед практичних фахівців, оскільки ЗМІ виступають як керівник населення до достовірної та об’єктивної інформації.

Слід зазначити, що в Україні під час війни фіксується велика кількість кримінальних правопорушень, які можна розділити на дві категорії: ті, які вчиняються російськими окупантами на території України (геноцид, вбивства, зґвалтування тощо), і ті, які вчиняють громадяни України (мародерство тощо). Об’єктивне та своєчасне повідомлення про ці протиправні дії допомагає швидко встановити

винних, зібрати докази і притягнути їх до кримінальної відповідальності.

У той же час, сучасні умови вимагають збалансованого підходу, який дозволяв би правоохоронним органам та представникам ЗМІ виконувати свої функції без перешкод і корисно співпрацювати. Важливо також враховувати, що відносини між цими двома сторонами визначають можливість отримання та поширення достовірної інформації із перших джерел, а не через посередників або непідтверджені коментарі.

Слід зауважити, що законодавчі норми України, а також міжнародно-правові стандарти, встановлюють конкретні обмеження для поширення певних інформаційних даних під час досудових стадій розслідування. У даному випадку ми маємо на увазі збереження конфіденційності досудового слідства, яка підпадає під захист відповідно до законодавчих норм різних сфер – кримінального права, кримінального процесуального права, а також Закону України «Про прокуратуру». Однак, у зв'язку з нагальними потребами в запобіганні злочинності в умовах воєнного стану, представники правоохоронних органів намагаються активно взаємодіяти з засобами масової інформації.

Один із напрямків такої співпраці полягає у розкритті діяльності правоохоронних органів під час розслідування кримінальних правопорушень, зокрема, які були вчинені в умовах воєнного стану. Розголошення інформації про роботу правоохоронних органів через телебачення сприяє реалізації концепції соціальної інформації, яка включає три ключові аспекти: освітній (розповсюдження повідомлень, що є основою корисної інформації), пізнавальний (формування уявлення на основі отриманої логічної та прагматичної інформації) і передбачувальний (розповсюдження відомостей, що стосуються майбутнього, можливого прогнозу).

Телевізійні програми, які розповідають про роботу поліції, сприяють створенню соціального контексту та розширюють розуміння глядачів. Вони допомагають громадянам розширити свій світогляд, змінити свої переконання і звички. Ці програми також сприяють об'єднанню суспільства навколо актуальних проблем і національних інтересів, стимулюють обговорення соціальних потреб, зокрема, діяльності правоохоронних органів, і сприяють формуванню гуманістичних поглядів.

Телебачення може виступити як платформа для влади, де вона може розповісти громадянам про свою політику та мобілізувати прихильників.

Правоохоронні органи повинні постачати інформацію ЗМІ щодо своєї діяльності у виявленні злочинців і розкритті кримінальних правопорушень, і суспільство має право на отримання цієї інформації для забезпечення власної безпеки та запобігання злочинам. Однак як поліцейські, так і представники ЗМІ повинні дотримуватися вимог законодавства, щоб точно визначити обсяг інформації, що розголошується, надаючи інформацію, яка має загальний інтерес, і утримуючи конфіденційну інформацію щодо досудового розслідування.

Важливо відзначити, що в умовах воєнного стану в Україні, зокрема в місті Ірпінь на Київщині, після звільнення від російських окупантів виникла проблема мародерів. Управління територіальної оборони міста швидко вирішило підсилити співпрацю з поліцією для забезпечення цілодобового патрулювання вулиць. Правоохоронці та захисники міста щоденно затримували мародерів із вже награбованим майном місцевих жителів, включаючи гроші, ноутбуки, телефони, ключі від автомобілів і коштовності. Цих осіб передавали поліції, але до розгляду справи мародерів також залучали до робіт із прибирання міста [76].

Правоохоронці та територіальна оборона активно та оперативно розголошували свою діяльність через засоби масової інформації. Олександр Маркушин, який одночасно є мером Ірпеня та керівником територіальної оборони, публікував майже кожен випадок мародерства в місті, закликаючи людей не використовувати чужий горе. Ці повідомлення досить швидко попадали в місцеві ЗМІ. Ми вважаємо, що такі дії мають позитивний вплив на правосвідомість громадян і викликають негоду до тих, хто зловживає ситуацією та вчиняє крадіжки в умовах війни.

Важливо підкреслити, що в контексті співпраці представників ЗМІ та правоохоронних органів у запобіганні злочинності в умовах воєнного стану, особливо важливою стає роль прес-служб. Ми погоджуємося з думкою М. Т. Андрійчука та Т. С. Андрійчука, що їх основна функція у таких ситуаціях – координація зусиль між правоохоронцями та журналістами, щоб забезпечити безпеку громадян і представників ЗМІ, дозволяючи поліцейським забезпечувати

громадянську безпеку і журналістам якісно виконувати свої редакційні завдання [9].

З метою покращення співпраці між ЗМІ та правоохоронними органами, з 2017 року в Головному управлінні Національної поліції у м. Києві був створений поліцейський відділ превентивної комунікації. Цей відділ був створений спеціально для роботи під час різноманітних масових подій, незалежно від їх політичного, спортивного, розважального або культурного спрямування. Його завданням є запобігання виникненню конфліктних ситуацій, пояснення дій поліції та зупинення агресивних громадян за допомогою ненасильницьких методів ще до вчинення кримінальних правопорушень.

Проте журналісти висловлюють свої обґрунтовані обурення щодо цих нововведень, оскільки вони вважають, що прес-служби не виправдовують очікувань, які до них пред'являють. Наприклад, журналіст О. Єльцов стверджує, що направлення представників ЗМІ до прес-служб є «частковим обмеженням доступу до інформації та потенційним засобом приховування її». За словами Єльцова, інформацію про події повинні надавати безпосередні представники правоохоронних органів, які можуть розповісти про неї «живцем» та забезпечити всю необхідну інформацію.

З іншого боку, представники правоохоронних органів висловлюють обурення некомпетентністю деяких журналістів і великою кількістю запитів на інформацію, яку можна легко знайти у відкритих джерелах. Прес-служби витрачають значний час на надання інформації відповідно до законодавства. У майбутньому цю проблему слід ретельніше дослідити і запропонувати ефективні рішення.

З огляду на активну участь працівників правоохоронних органів у розповсюдженні інформації про їх діяльність важливо розглядати можливість зміни практики залучення до ЗМІ. Слід розширити спектр участі у медійних заходах та підвищити якість інформування громадськості. Це особливо стосується своєчасного, об'єктивного та повного інформування суспільства про важливі справи та заходи правоохоронних органів. Важливо висвітлювати інформацію щодо результатів, які сприяли відновленню законності та порядку. Потрібно реагувати оперативно на критику та повідомлення про діяльність правоохоронних органів, особливо з урахуванням того,

що багато людей отримують інформацію через телевізійні та радіо передачі.

Все вищезазначене свідчить про недоліки в законодавчому регулюванні взаємодії між ЗМІ і правоохоронними органами та підкреслює організаційний аспект цієї взаємодії.

Один із способів взаємодії правоохоронних органів і ЗМІ у запобіганні злочинності в умовах воєнного стану – це акредитація журналістів у правоохоронних органах. Згідно з діючим законодавством щодо друкованих ЗМІ, Національна поліція України має право проводити акредитацію журналістів з метою зміцнення співпраці між правоохоронними органами та ЗМІ, освіти громадян України щодо законної діяльності поліції та боротьби зі злочинністю. Акредитовані журналісти мають право вільного доступу та перебування на території та в приміщеннях МВС та Національної поліції за наявності акредитаційної картки з 9.00 до 20.00 годин, крім вихідних. ЗМІ також можуть акредитувати своїх журналістів у правоохоронних органах за їхньою згодою. Висвітлення таких подій сприяє позитивному сприйняттю громадськістю та покращує імідж правоохоронних органів.

Ще одним способом взаємодії правоохоронних органів і ЗМІ у запобіганні злочинності в умовах воєнного стану є проведення спільних благодійних акцій. Це дозволяє привернути увагу громадськості до проблем правоохоронної діяльності, запобігання порушенням закону, та залучити додаткові фінансові ресурси для підтримки правоохоронних органів і програм профілактики.

Спільні видання рубрик, спільні теле- та радіопрограми є ще одним важливим напрямком взаємодії між правоохоронними органами і ЗМІ у запобіганні злочинності в умовах воєнного стану. Зокрема, радіомовлення є надзвичайно потужним ЗМІ, оскільки передає лише звук та може доносити інформацію на будь-які відстані миттєво. Радіо вимагає мінімальних технічних засобів для сприйняття та має великий потенціал для інформування громадськості про діяльність правоохоронних органів.

Проведення «прямих ліній» та «прямих ефірів» відіграє важливу роль в роботі поліції. Керівники служб та підрозділів Національної поліції взаємодіють з ЗМІ, де вони обговорюють питання правоохоронної діяльності, розповідають про розкриття тяжких злочинів, а також відповідають на питання громадян прямо у

редакціях газет. Після таких інтеракцій інформація публікується у ЗМІ.

Сьогодні практикується проведення «круглих столів» та брифінгів, на яких обговорюються питання боротьби зі злочинністю в конкретних регіонах та забезпечення громадської та особистої безпеки громадян. Для участі в таких заходах запрошуються працівники поліції, представники громадських організацій, видатні фахівці та вчені тощо. Результати цих дискусій пізніше висвітлюються у ЗМІ.

Ще однією формою співпраці є зустрічі працівників поліції з редакціями, на яких обговорюються різні аспекти діяльності правоохоронних органів, практика застосування законів та проблеми, з якими стикаються поліцейські. З цих зустрічей також готуються матеріали для публікації.

Взаємодія між правоохоронними органами та ЗМІ дозволяє їм більш ефективно використовувати свої інтелектуальні та матеріальні ресурси, оптимізувати прийняття рішень в процесі розслідування, підвищувати ефективність різних правових, профілактичних та превентивних заходів, а також формувати адекватну громадську думку щодо роботи правоохоронних органів.

Один із яскравих прикладів такої взаємодії в умовах воєнного стану – створення Telegram-чат-боту «Є-ворог», який дозволяє повідомляти про окупантів та осіб, причетних до геноциду українського народу. Цей чат-бот допомагає запобігти поширенню фейкової інформації та забезпечує отримання правдивої інформації. Також інші сервіси та онлайн-ресурси сприяють пошуку зниклих людей та надають можливість зв’язку між родичами та близькими у важкий час конфлікту.

Незважаючи на значні успіхи у встановленні взаємодії між правоохоронними органами та засобами масової інформації, існують деякі поширені проблеми, які стосуються цієї співпраці:

1. Недостатня нормативно-правова база, зокрема, в галузі чіткого регулювання відносин між правоохоронними органами та ЗМІ.

2. Відсутність в правоохоронних органах практики ефективної взаємодії із ЗМІ. Зазвичай відповіді від органів влади на публікації ЗМІ мають стандартний характер, і прес-конференції часто обмежуються формальними заявами.

3. Обмежений доступ журналістів до керівництва правоохоронних органів, що часто ускладнює можливість отримання швидкого коментаря для ЗМІ.

4. Недостатня оперативність правоохоронних органів у розповсюдженні інформації про свої заходи. Коментарі на актуальні теми іноді з'являються у прес-службах з певною затримкою.

Отже, наступним важливим кроком є необхідність реформування законодавства щодо взаємовідносин між правоохоронними органами та ЗМІ. Це передбачає створення механізму для ефективної співпраці і мінімізації матеріальних та інших витрат для забезпечення успішної взаємодії між цими сторонами.

Крім того, Україні необхідно розробити ефективну інформаційну політику, спрямовану на інформування громадян та забезпечення їх розуміння причин вчинення кримінальних правопорушень в інформаційному просторі. Це також включає підвищення рівня медіаграмотності, щоб громадяни могли відповідати на спроби маніпулювання ними через інформаційні потоки. Такі заходи сприятимуть побудови системи захисту кожної людини від негативного впливу інформаційної злочинності.

Для поліпшення взаємодії у відносинах між правоохоронними органами та засобами масової інформації в умовах воєнного стану, ми вважаємо, що є необхідними такі підходи:

1. Перший захід полягає у створенні та прийнятті нормативно-правового акта, який регламентуватиме взаємовигідні аспекти співпраці між правоохоронними органами та представниками ЗМІ у сфері запобігання злочинності, особливо в інформаційному просторі. Важливо зауважити, що Україна вже втратила діючу Інструкцію «Про взаємодію правоохоронних та інших державних органів України у боротьбі із злочинністю», яка була прийнята у 1994 році. Таким чином, прийняття нового правового акта стає актуальною необхідністю у контексті сучасних реформ у країні.

2. Другий важливий захід полягає в тому, що співпраця правоохоронних органів має здійснюватися з журналістами, які розуміються у сфері юриспруденції. Це допоможе зменшити можливість неправильного трактування юридичних термінів і подій, а також перекручування відповідних фактів.

У підсумку, можемо виділити такі рекомендації щодо взаємодії зі ЗМІ:

1. Відкритість та прозорість діяльності правоохоронних органів є невід'ємною частиною сучасного демократичного суспільства, і вона вимагає налагодженої комунікації зі ЗМІ.

2. Для досягнення цієї мети важливо залучати як міжнародних, так і національних експертів, включаючи представників бізнес-середовища, оскільки ефективна діяльність має належно висвітлюватися в ЗМІ. Важливо враховувати бренд-стилістику, впізнаваність, якість роботи у соціальних мережах, ближчу до бізнес-стандартів.

3. Не боятися залучати безпосередніх виконавців роботи до спілкування з журналістами.

4. Від журналістів і ЗМІ також важливо очікувати вищого рівня професіоналізму.

Отже, ці рекомендації сприятимуть покращенню ефективності взаємодії між правоохоронними органами та ЗМІ в умовах воєнного стану та сприятимуть подальшій роботі над цим питанням.

Особливу увагу у межах нашого дослідження слід приділити запобіганню кібершахрайству. З урахуванням сучасного етапу цифрової трансформації в усіх сферах фінансового життя у всьому світі, а також кризових явищ в економіці, стає очевидним, що проблема фінансового шахрайства стає все більш актуальною як для фізичних, так і для юридичних осіб. Кожен рік, відповідно до розвитку цифрових технологій, з'являються нові види та методи шахрайства в галузі фінансових ресурсів, що надає фінансовому шахрайству всі можливості для швидкої адаптації до сучасних умов підприємницької діяльності. Зокрема, фінансове шахрайство є поширеним явищем на підприємствах. За результатами проведених досліджень в Україні приблизно половина підприємців хоча б раз ставали жертвою шахраїв. Це призводить до значної кількості негативних наслідків для функціонування суб'єктів господарювання, включаючи погіршення репутації підприємства та підрив його фінансового стану в цілому. Зараз шахраї володіють широким спектром методів, тоді як правоохоронці лише розробляють механізми запобігання та виявлення зловживань, і більшість українських компаній не проводять розслідування випадків фінансового шахрайства [337, с. 71].

Це питання набуло особливої актуальності під час повномасштабної війни в Україні, оскільки кібершахрайство почало поширюватися з надзвичайною інтенсивністю. Використовуючи

воєнний стан та скрутне становище українців, зловмисники спритно маніпулюють емоційним станом людей, здійснюючи шахрайські дії для незаконного збору коштів.

За минулий рік, загальна сума збитків, завданих банкам, підприємствам та іншим клієнтам через незаконні дії з платіжними картками, становила 481 мільйон гривень. Це на 46 % більше, ніж у 2021 році. Кількість незаконних операцій з платіжними картками, що спричинили збитки, зросла на 8 % протягом минулого року. Тому питання запобігання кібершахрайству у фінансовому секторі набуває особливої важливості в наші дні.

Внаслідок воєнних подій в Україні 85 % підприємств змушені приймати заходи з оптимізації своїх бізнес-процесів. З цієї кількості, 1 % компаній припинили свою діяльність і, ймовірно, не зможуть відновити її в найближчому майбутньому, а 35 % призупинили свою роботу в очікуванні покращення економічної ситуації. Ці результати базуються на дослідженні, яке провела компанія Gradus Research за замовленням Київської школи економіки [305]. Ця ситуація не лише становить загрозу для економіки країни та розвитку підприємницької діяльності, але також створює додаткові можливості для корпоративного шахрайства в тих випадках, коли гарантування надійності систем внутрішнього контролю не є пріоритетним завданням. Проте такі дії, які відбуваються в умовах, коли бізнес вже страждає від кризи, можуть виявитися руйнівними для нього.

Для оцінки рівня шахрайства з платіжними картками зазвичай аналізують не тільки загальну суму збитків, але і порівнюють її з загальною сумою усіх операцій з платіжними картками. Зараз ця сума збитків є не набагато більшою, ніж у 2021 році. Таким чином, можемо прийти до висновку, що в минулому році сума збитків від шахрайства зростала пропорційно зростанню загальної суми операцій з платіжними картками в українських банках.

Якщо розглядати динаміку рівня шахрайства з платіжними картками за місцем проведення операцій, то на 1 мільйон гривень операцій сума збитків від шахрайських дій у 2022 році порівняно з 2021 роком зменшилася в фізичних пристроях (у торговельних мережах – з 40 гривень до 16 гривень, в банкоматах – з 29 гривень до 5 гривень). Проте рівень шахрайства в Інтернеті збільшився з 114 гривень до 133 гривень. Загалом, у минулому році 86 % випадків шахрайства відбувалися в Інтернеті, в той час як тільки 14 % – через фізичні пристрої (торговельна мережа, банкомати). Що стосується

суми збитків від незаконних дій, то 94 % припадає на Інтернет, 4 % – на торговельну мережу і 2 % – на банкомати [344].

Таким чином, в галузях, де використовуються фізичні платіжні картки, такі як торговельні мережі, банкомати та самообслуговувальні пристрої, на даний момент здійснення операцій вважається більш безпечним. Оскільки підробити фізичну картку для використання в банкоматі або торговельній мережі є складнішим завданням, ніж викрасти дані клієнта і здійснити операцію в Інтернеті.

Але важливо відзначити, що, навіть якщо механізми платіжного шахрайства залишаються тими ж під час війни, з'являються нові сценарії. Найпоширенішим серед нових сценаріїв є фейкова соціальна допомога від державних або міжнародних організацій. З середини 2022 року і до сьогоднішнього часу відзначається найвищий рівень активності в цьому напрямку. Щодня в Україні приблизно 10 000–15 000 громадян переходять за посиланнями на шахрайські фішингові веб-сайти і, відповідно, стають жертвами шахраїв. [344].

Шахраї, використовуючи шкідливі фішингові ресурси, намагаються обдурити громадян та здобути доступ до їхніх фінансових даних. Ці веб-сайти в основному маскуються під урядові портали, такі як «Дія», «Є-Допомога», або імітують сайти українських банків, міжнародних організацій та відомих платіжних сервісів.

Людина, не розуміючи, що це фейковий сайт, розголошує на ньому конфіденційну інформацію, яку не слід розголошувати, таку як CVV-код, пін-код, логін та пароль для доступу до Інтернет-банкінгу тощо. Після цього зловмисники просто викрадають гроші з її рахунків або психологічно тиснуть на особу, вимагаючи виконати платіж на користь шахраїв та інше.

У 2022 році Національний банк України виявив понад 4500 таких фішингових ресурсів. З початку 2023 року і до сьогоднішнього дня було виявлено понад 11 000 подібних шахрайських доменів. В середньому кожен день виявляється більше 100 таких шахрайських ресурсів. Операторами більшості цих шахрайств є групи з росії. Приблизно дві третини виявлених фішингових сайтів (68 %) мають походження з росії. Отже, крім військової агресії, проти нас ведеться гібридна війна у віртуальному просторі з використанням кібергруп росії. [344].

Це очевидно навіть з текстів фішингових повідомлень, які часто містять некоректний переклад, русизми і невірно вжиті слова.

Тому проблема запобігання кібершахрайству у фінансовому секторі на сьогодні є критично важливою і потребує негайного вирішення.

У цьому контексті Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України спільно з Національним банком України розпочали проєкт боротьби з кібершахрайством у фінансовому секторі.

Основною метою цього проєкту є посилення захисту громадян від кіберзлочинців, які значно активізували свою діяльність під час воєнного стану в Україні. Як вже відзначено, злочинці використовують фішингові кампанії для виманення даних, необхідних для доступу до банківських рахунків. Вони надають обіцянки, що відрізняються від актуальних новин, особливо тих, що стосуються надання державної та міжнародної фінансової допомоги громадянам, і також організовують фейкові збори коштів для підтримки Збройних Сил України.

Завданням цьому проєкту є зменшення кількості переходів користувачів на шахрайські веб-сайти шляхом перенаправлення їх на сторінку з попередженням, що сайт створений зловмисниками. Результати вражають: лише за перший місяць було зафіксовано приблизно 120 тисяч унікальних переходів на цю сторінку. Іншими словами, десятки тисяч громадян України щомісяця будуть захищені від незаконних дій шахраїв [37].

Також слід враховувати, що у 2022 році в Національному координаційному центрі кібербезпеки була утворена робоча група, в яку увійшли представники державних органів та провайдери з найбільшою інфраструктурою. Було успішно протестовано роботу системи захисту від фінансового фішингу. Першим великим провайдером, який активно долучився до цього проєкту, стала компанія «Київстар», яка завжди надає велику увагу питанням кібербезпеки та захисту своїх абонентів від кіберзагроз.

Аналіз активності хакерських груп, що займаються подібними шахрайствами, показує, що вони діють не лише в Україні, але й у країнах Європейського Союзу. Тому зараз проводяться переговори щодо обміну інформацією з відповідними органами з країн-партнерів, до яких після початку повномасштабного вторгнення в Україні виїхала велика кількість українців. [299].

Отже, запобігання кіберзлочинності передбачає впровадження різних заходів, як загальнодержавних, так і спеціалізованих, що включають економічні, ідеологічні, правові, та виховні заходи. Україна має численні платформи для інформування громадян про шахрайські схеми та способи захисту від кібершахрайства. Національний банк України, спільно з партнерами, активно інформує громадян про заходи проти платіжного шахрайства через спеціальну веб-сторінку #ШахраїГудбай, яка містить докладну інформацію про кампанію та правила безпеки в онлайн-середовищі. Важливо підкреслити, що боротьба з кіберзлочинністю вимагає використання специфічних засобів і підходів.

Паралельно варто розглядати міжнародний досвід у цій сфері. Для боротьби проти незаконних вторгнень в електронні інформаційні ресурси потрібно встановити механізми оперативного обмеження (блокування) певних інформаційних ресурсів і впровадити особливі умови для проведення обшуку та арешту електронних доказів, зокрема, забезпечити можливість копіювання і збереження інформації операторами, телекомунікаційними провайдерами та власниками веб-сайтів з метою забезпечення цілісності цих даних. ООН та інші міжнародні організації, які сприяють мирним відносинам і дипломатії, відіграють важливу роль у боротьбі з кіберзлочинністю та кібершахрайством. Прийняття правових актів в цій сфері має на меті підтримку інформаційної безпеки та запобігання кіберзлочинності.

Висновки до Розділу 3

1. Запобігання кіберзлочинності дійсно є актуальною та складною проблемою у сучасному світі. Зростання кількості та складності кіберзлочинів вимагає постійного оновлення та адаптації стратегій та заходів з кібербезпеки. Основні причини зростання кіберзлочинності включають в себе:

1) Технологічний прогрес: швидкий розвиток інформаційних технологій створює нові можливості для кіберзлочинців, такі як атаки на великі мережі та користувачів, використання розширених методів шифрування та анонімізації.

2) Анонімність в Інтернеті: інтернет надає злочинцям можливість діяти анонімно, що ускладнює їх ідентифікацію та затримання.

3) Глобальний характер кіберзлочинності: кіберзлочини можуть бути вчинені з будь-якої точки світу та спрямовані проти будь-якої іншої країни. Це ускладнює судове переслідування та співпрацю між державами.

Щодо ситуації в Україні, конфлікт з росією дійсно призвів до зростання кіберзлочинності, включаючи кібератаки та кібершпигунство. Цей конфлікт підкреслює важливість кібербезпеки для захисту національних інтересів та інфраструктури.

2. На міжнародному рівні запобігання злочинності у сфері інформаційних технологій здійснюється на належному рівні: сформовані універсальні та регіональні механізми запобігання цьому небезпечному явищу. Поряд з тим, сучасний стан міжнародного співробітництва свідчить про наявність нових загроз, які значно впливають на стан запобігання злочинності у цій сфері. Тому необхідно враховувати такі загрози і адаптувати законодавство як на міжнародному рівні, так і внутрішньодержавне.

3. Дослідження проблем, пов’язаних із координацією дій спеціальних органів держав для запобігання кіберзлочинності та розробки сучасних механізмів боротьби з нею, є одним із пріоритетних напрямків для кожної держави. Зрозуміло, що кіберзлочинність має прямий вплив на глобалізацію інформаційних процесів та розвиток глобальних телекомунікаційних мереж.

Ефективна боротьба з кіберзлочинністю потребує не лише узгодження кримінального законодавства на міжнародному рівні, але і систематизації та адаптації процедурних заходів для співпраці у сфері запобігання кіберзлочинам. На сьогоднішній день не існує єдиної міжнародної системи для боротьби з кіберзлочинністю, яка б використовувалася всіма країнами світу. Для оцінки готовності інформаційних систем країн до кібератак був використаний рейтинг McAfee. Результати показали, що тільки три країни, а саме Швеція, Ізраїль і Фінляндія, здобули найвищий бал 4,5 з 5, в той час як ще вісім країн, включаючи США, Великобританію, Францію та Німеччину, отримали другий результат 4 бали. Польща зайняла четверте місце з 3 балами. Деякі країни, зокрема Україна, не були включені до цього дослідження.

4. Необхідність у посиленні кримінальної відповідальності за порушення у галузі інформаційних технологій була актуальною вже протягом тривалого періоду. Зміни до законодавства включають в

себе розширення повноважень правоохоронних органів для розслідування кіберзлочинів, які передбачені статтями 361 і 361-1 Кримінального кодексу України. Заходи, спрямовані на посилення санкцій та додаткове криміналізування окремих дій, можуть обмежити можливість потенційних злочинців вчиняти нові кримінальні правопорушення.

Надзвичайно важливим, на нашу думку, є впровадження відповідальності за вищезазначені кримінальні правопорушення, вчинені під час воєнного стану. За такі протиправні дії повинні передбачатися суворі санкції, оскільки обставини в країні вимагають цього. Особа, яка завдає шкоди національним інтересам України у кіберпросторі і таким чином допомагає агресору в цій війні, повинна нести відповідальність, аналогічно воєнним злочинцям.

РОЗДІЛ 4
ЗАРУБІЖНИЙ ДОСВІД ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ В УКРАЇНІ

4.1. Досвід окремих зарубіжних країн щодо запобігання злочинності у сфері використання інформаційних технологій

Сьогодні суспільство переживає стрімкий прогрес автоматизації, інформатизації та комп'ютеризації у всіх сферах. Ці процеси відкривають нові перспективи для розвитку культури, освіти, науки й економіки кожної країни, а також сприяють швидкій взаємодії з іншими країнами та міжнародними організаціями. Однак розповсюдження інформаційних технологій має й негативні наслідки, оскільки воно відкриває можливості для кримінально протиправної поведінки. Комп'ютерні системи надають нові, дуже вдосконалені можливості для вчинення раніше невідомих порушень та традиційних кримінальних правопорушень, але за допомогою нетрадиційних засобів.

У цьому контексті терміни «кіберзлочинність», «кібершахрайство», «хакери», «комп'ютерний злом» та «крадіжка машинного часу» вже не є невідомими поняттями. Сьогодні злочинність у сфері інформаційних технологій є однією з найдинамічніших категорій суспільно небезпечних порушень. Неможливо заперечити, що швидке зростання поширення такої злочинності та постійне збільшення її суспільної небезпеки стали негативним результатом такого важливого суспільного процесу, як інформатизація.

У нашій країні кількість правопорушень у сфері інформаційних технологій не є значною у порівнянні з країнами, такими як США, Великобританія, Німеччина та інші, де відбуваються надзвичайно великі масштаби таких порушень. Однак існує тенденція до зростання цього виду злочинності, що підтверджують статистичні дані.

Крім цього, злочинність у сфері інформаційних технологій відзначається високим рівнем латентності. За різними оцінками, правоохоронним органам відомо лише про 10–20 % таких кримінальних порушень [26]. Все це пояснюється складністю ідентифікації осіб, які здійснюють кримінальні правопорушення у

галузі інформаційних технологій, відсутністю єдиної методології розслідування та формування системи запобігання цього виду злочинності.

На думку експертів, зростання кількості кримінальних правопорушень пояснюється особливостями віртуального простору, оскільки злочинці не бачать своїх потенційних жертв, яких «вони обрали для атаки». Таким чином, злочинці вірять у свою анонімність та відсутність безпосередньої небезпеки виявлення та переслідування. Згідно з практикою, коли злочинці зіткнуться з опором технічних систем захисту від несанкціонованого доступу до комп'ютерних систем, вони шукають нову інформацію та вдосконалюють свої знання про способи та методи здійснення кримінального правопорушення. Важливо відзначити, що найбільш поширеними мотивами вчинення кримінальних правопорушень у сфері інформаційних технологій є матеріальна користь та хуліганські наміри, але можливі також мотиви зацікавленості, бажання помсти, а також випадки вчинення для приховування іншого кримінального правопорушення [22].

У той же час спостерігається збільшення випадків втручання у функціонування комп'ютеризованих систем, які обслуговують сектор економіки держави. Відзначається зростання кількості атак на об'єкти, що відносяться до «критичної інформаційної інфраструктури» країни. Більшість «кіберінцидентів», які були зафіксовані в звітах Центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку, не мають чіткого відображення в національному законодавстві. Багато з них можна вважати умовними формами вчинення кримінального правопорушення, який передбачений статтею 361 Кримінального кодексу України. [153].

Швидкий прогрес комунікаційних мереж, інформаційних технологій та всеосяжної комп'ютеризації викликав еволюційні зміни у кримінальному середовищі, як на рівні окремих країн, так і в світовому співтоваристві. Недостатній соціальний контроль призвів до того, що Інтернет практично безкарно використовується злочинцями як місце та основний інструмент для здійснення різних незаконних дій, включаючи традиційні (шахрайство, крадіжки) та інші – викрадення та продаж конфіденційної інформації, шахрайства в геймерському середовищі, а також розповсюдження предметів та послуг, які були вилучені з легального обігу (наркотики, дитяча порнографія). Особливу загрозу представляють кіберекстремізм і

його крайня форма – кібертероризм, який полягає в дезорганізації роботи інформаційних систем з метою створення загрози для життя людей, завдання значної матеріальної шкоди або настання інших суспільно небезпечних наслідків. Ці дії вчиняються з метою порушення громадської безпеки, залякування населення, впливу на прийняття рішень державними органами та загрози вчинення таких дій з тією ж метою.

Як ми уже відмічали, запобігання злочинності у сфері інформаційних технологій є однією з найбільш актуальних та складних проблем у галузі кримінології. Умови високої латентності, зростання кількості кіберзлочинів та постійне вдосконалення інформаційних технологій, які надають нові можливості для вчинення злочинів, вимагають кардинально нових підходів до запобігання порушень у віртуальному просторі та їх загроз для глобальних інформаційних мереж та суспільства загалом.

Аналізуючи кіберзлочинність в Україні, можна зробити такі висновки:

– кіберзлочинність є окремим видом злочинності, який існує паралельно з насильницькими, корисливими, корупційними, екологічними та іншими видами кримінально протиправних діянь;

– вона тісно пов’язана з іншими видами злочинності, оскільки кримінальні правопорушення у сфері інформаційних технологій часто використовуються як засіб удосконалення інших кримінальних правопорушень (крадіжки, вимагання, шахрайства та інші);

– цей вид злочинності характеризується високотехнологічним підходом, спричиненим використанням ІТ-технологій, інформаційно-телекомунікаційних мереж, комп’ютерних пристроїв, носіїв комп’ютерної інформації та інших засобів для вчинення кримінально протиправних дій;

– кіберзлочинність має високий рівень латентності, що означає, що відсоток розкриття цих кримінальних правопорушень дуже низький, від декількох десятків до декількох тисяч відсотків, залежно від виду кримінального правопорушення. Це пов’язано з різними об’єктивними факторами, такими як небажання потерпілих звертатися до правоохоронних органів, неочевидність кіберзлочинів для більшості громадян через їх вчинення в віртуальному середовищі, а також складність виявлення цих кримінальних правопорушень при обмеженому числі фахівців у правоохоронних органах;

– має організований характер і тісно пов’язана з організованою злочинністю, оскільки значна кількість кіберзлочинів (наприклад, DDoS-атаки, Е-банкінг, фішинг, створення ботів тощо) здійснюються злочинними групами;

– має «професійний» характер, оскільки особи, які вчиняють кіберзлочини, спеціалізуються саме на цьому типі злочинності, отримують дохід від кримінально протиправної діяльності, володіють необхідними знаннями, вміннями та навичками в сфері ІТ-технологій для вчинення кримінальних правопорушень. Вони дотримуються певних правил, законів, понять і термінології, що дозволяє їм спілкуватися, обмінюватися досвідом і знаходити однодумців;

– характеризується транскордонністю, оскільки кіберпростір існує поза державними кордонами і є загальнодоступним. Це дозволяє злочинцю, який перебуває на території однієї держави, вчиняти кримінально протиправні дії щодо осіб, що перебувають в іншій державі;

– має транснаціональний характер, оскільки кіберзлочинці з комп’ютерного «андеграунду», щоб отримати незаконний дохід та спростити вчинення кримінально протиправних дій на території різних держав, об’єднуються в міжнародні незаконні групи, незалежно від національності [171, с. 356];

– перебуває в процесі постійного розширення та розвитку, що зумовлено постійним удосконаленням існуючих технологій та створенням нових ІТ-рішень. Цей розвиток відбувається за умов залучення нових учасників до інформаційних процесів та поширення кіберпростору завдяки збільшенню кількості користувачів мережі Інтернет, мобільних комп’ютерних пристроїв та поступовому переходу до електронного документообігу більшої кількості організацій, підприємств і установ.

– приймає риси економічної злочинності, оскільки більшість кіберзлочинів спостерігається в банківсько-фінансовому та корпоративному секторах (наприклад, інтернет-банкінг, банківський фішинг, кібервимагання тощо), а дії злочинців спрямовані на винесення доходів (прибутку).

– перетворюється на злочинність політичного спрямування, пов’язану з активізацією незаконних дій у кіберпросторі з боку представників хакерського руху, спецслужб та силових структур зарубіжних держав, міжнародних екстремістських та терористичних

організацій (наприклад, DDoS-атаки на урядові веб-сайти, кібершпигунство відносно інформаційних ресурсів органів державної влади, правоохоронних органів, підприємств оборонно-промислового комплексу, дипломатичних представництв та інше). [202].

Повністю погоджуючись з поглядами О. В. Таволжанського, хочемо зазначити, що для надання ефективності або удосконалення впровадження національних стратегічних підходів до розглянутого питання, можна взяти за основу позитивний досвід діяльності урядових та непублічних організацій інших країн, а також міжнародних установ, і врахувати їхні досягнення у протидії загрозам інформаційній безпеці. У сучасних умовах важко уявити захищену країну, яка не б займалася своїми секторами зовнішньої безпеки та не адаптувалася до викликів нашого часу. Ніяка війна, чи відкрита, чи прихована, не відбувається без використання кіберзброї, використання потенціалу мережі Інтернет як кіберресурсу у військових цілях на сьогодні є невід'ємною складовою. У політиці провідних країн постійно розробляються передові заходи для протистояння загрозам у кіберпросторі, відбувається коригування внутрішньої інформаційної політики та удосконалення методів кібербезпеки. [304, с. 155]. Саме це спонукає нас до активного вивчення злочинності у сфері інформаційних технологій та необхідності вжиття заходів для запобігання цьому негативному явищу.

Вчені, такі як П. Д. Біленчук, Л. Д. Варунц, М. І. Малій, В. В. Марков, О. В. Таволжанський та інші проводили кримінологічні дослідження за зарубіжним досвідом у запобіганні злочинності у сфері інформаційних технологій.

При вивченні цього питання ми звернулися до досвіду найрозвиненіших країн світу. Порівняльно-правовий аналіз законодавства цих країн і України свідчить про те, що за кордоном у більшості держав створена комплексна система органів для забезпечення кібербезпеки. Наприклад, у США існує Управління національної безпеки (Department of Homeland Security), в межах якого працює спеціальний кібербезпековий департамент, що відповідає за безпеку високотехнологічних систем країни. Також існує Кіберкомандування, яке веде спеціальні підрозділи з метою розвідування мереж, захисту власних мереж, блокування та дезорганізації структур супротивника в кіберпросторі.

В Канаді запобігання комп'ютерній та телекомунікаційній злочинності забезпечується діяльністю підрозділу Королівської

канадської кінної поліції (далі – КККП). Цей підрозділ спеціалізується на розслідуванні та виявленні правопорушень, пов'язаних з комп'ютерною діяльністю та телекомунікаціями. Секція захисту інформаційних технологій займається захистом федеральних державних комп'ютерних центрів, а також надає консультації та готує персонал для роботи з комп'ютерним захистом у приватному секторі. Працівники цього підрозділу надають підтримку поліцейським у розслідуванні злочинів, пов'язаних з комп'ютерними системами. Оскільки інформаційна система дозволяє передавати повідомлення між терміналами майже миттєво, в Канаді функціонує близько 2500 точок доступу, до яких належать близько 1285 федеральних і провінційних поліцейських відділень. 1180 спеціалізованих відділень КККП забезпечені підключенням до системи. [79, с. 127].

Безперечно, цей напрямок діяльності поліції є важливим, оскільки економічні втрати вже досягли широких масштабів, деякі злочинці діють на міжнародному рівні у складі організованих груп. Одному державному органу складно запобігати злочинність у сфері інформаційних технологій.

У зв'язку з цим, науковці у галузі кримінології вказують на те, що канадське законодавство щодо визначення злочинності у сфері інформаційних технологій є суперечливим і потребує удосконалення. Оскільки завдання, які стоять перед поліцією у боротьбі зі злочинністю у цій сфері, мають міжнародний характер і не є специфічними для Канади, її представники активно взаємодіють з іншими країнами та Інтерполом для вдосконалення відповідного законодавства. Розкриття комп'ютерних кримінальних правопорушень є складним завданням, особливо через обмежений часовий ресурс. Оскільки передача даних може бути здійснена майже миттєво, часто безуспішно вдаються до спроб знайти будь-які докази, які підтверджують порушення міжнародного законодавства. За даними Королівської канадської кінної поліції (КККП), на сьогодні численні комп'ютерні кримінальні правопорушення вчиняються неповнолітніми, які ще не досягли дванадцятирічного віку. Відповідно до кримінального кодексу Канади, для встановлення кримінальної відповідальності необхідно підтвердити несанкціоноване використання комп'ютерної системи та намір особи заподіяти шкоду своїми діями. Такий підхід вимагає чіткого

визначення параметрів доступу до комп'ютерної техніки з метою попередження порушень.

Важливо враховувати відомості про осіб та обмеження, пов'язані з параметрами доступу, у тому числі можливість працівників випробовувати програми. Експертну консультацію щодо можливих неправомірних дій у цьому контексті може надати Міністерство юстиції або відповідний підрозділ Королівської канадської кінної поліції (КККП) [198, с. 110].

Важливо відзначити, що розслідування випадків несанкціонованого дистанційного доступу до комп'ютерних мереж є складною технічною методикою, якою займаються спеціалізовані поліцейські відділи. У зв'язку з загрозою комп'ютерної злочинності та її зростаючим впливом на світове співтовариство, в рамках ООН регулярно проводяться симпозіуми з профілактики та припинення комп'ютерної злочинності. Фахівці відзначають програмні методи захисту інформації в колективно використовуваних комп'ютерних системах як один із шляхів удосконалення системи автоматичного контролю. Для запобігання та зменшення кримінальних правопорушень, пов'язаних з незаконним використанням телекомунікаційних систем на міжпровінційному, державному та міжнародному рівнях, спрямовані дії та управління контролю над економічними злочинами. Інформаційний центр надає допомогу поліцейським підрозділам у цьому напрямі [198, с. 110].

Діяльність поліції з виявлення та запобігання злочинності у сфері інформаційних технологій орієнтована на широкий спектр відносин з різними соціальними групами через засоби масової інформації, консультації з представниками громадськості, співпрацю з урядовими та управлінськими органами, громадськими організаціями та окремими громадянами. У цьому контексті поліція виступає як важливий партнер спільноти організацій, що борються зі злочинністю, зокрема в галузі кібербезпеки, та забезпечує дотримання прав людини та захист федеральних державних комп'ютерних центрів та приватного сектору [79, с. 203].

Ефективна протидія комп'ютерній злочинності вимагає поглибленого та добре організованого співробітництва між правоохоронними органами різних країн, включаючи співпрацю в рамках Інтерполу.

При аналізі досвіду країн Європи можна відзначити, що, як і у США, тут утворено єдину систему державних органів, кожен з яких

має свої специфічні повноваження у протидії злочинності у сфері інформаційних технологій.

Фахівці правоохоронних органів Франції виділяють дві основні форми цього типу злочинності. Одна з них – це суспільно небезпечні дії, пов'язані з незаконним відтворенням комп'ютерного програмного забезпечення, незаконним втручанням у автоматизовані системи обробки даних, вторгненням на веб-сайти, створенням та розповсюдженням шкідливих програм та інші.

Другий тип кіберзлочинів вважається більш складним і динамічним, і використовує глобальні інформаційні мережі. Сюди включають поширення веб-сайтів, які мають відношення до таких видів контенту: дитяча порнографія, торгівля наркотиками, расизм, ксенофобія, антисемітизм, терористична пропаганда, вказівки на приватне життя, інструкції з виготовлення вибухових речовин, обманлива реклама тощо [71].

Так, у Франції наявна система державних та недержавних установ, які спеціалізуються на запобіганні кіберзлочинності. Однією з відомих структур є Національна комісія з обчислювальної техніки та свобод (CNIL). Основна мета CNIL – захист особистих даних. У цифровому світі CNIL виступає регулятором у сфері особистих даних, надаючи підтримку фахівцям в кіберпросторі та сприяючи громадянам у контролі над своїми особистими даними та реалізації своїх прав. З початку 2004 року CNIL має право накладати санкції на компанії, які порушують Закон про інформатику, файли та свободи 1978 року [382].

Однією з аспектів запобігання злочинності у сфері інформаційних технологій є ініціатива, відома як «Верховний орган поширення творів і захисту прав в Інтернеті» (HADOPI). Ця організація намагається визначити та регулювати незаконне завантаження інформації. Конституційний суд країни схвалив вторинний варіант Закону щодо «триступеневої заборони доступу до мережі Інтернет» [382].

У 2015 році Франція ухвалила Національну стратегію забезпечення інформаційної безпеки. Ця стратегія спрямована на супровід переходу французького суспільства до цифрових технологій та вирішення нових викликів, пов'язаних зі зміною використання цифрових технологій та породженими цим загрозами. У ній визначено п'ять головних напрямків діяльності: забезпечення національного суверенітету, ефективна реакція на зловмисні дії в комп'ютерних системах і мережах; інформування широкого загалу;

перетворення інформаційної безпеки на конкурентну перевагу французьких підприємств; збільшення впливу Франції на міжнародній арені [28].

У додаток до стратегії включають таке:

1. Міністр Європейських та закордонних справ представив Міжнародну стратегію Франції у сфері інформаційних технологій у грудні 2017 року. Цей документ узагальнює всі стратегічні мети Франції у сфері інформаційних технологій у трьох ключових галузях: управління, економіка та безпека;

2. У лютому 2018 року був представлений Стратегічний огляд з кіберзахисту, складений генеральним секретарем з питань оборони та національної безпеки за дорученням прем'єр-міністра. Цей огляд визначає доктрину управління кіберкризами. Крім того, він пояснює мети національної стратегії з кіберзахисту, підтверджує ефективність французької моделі та акцентує основну відповідальність держави у цій галузі [73].

У франційській правоохоронній системі також діють відповідні суб'єкти, які займаються боротьбою зі злочинністю у сфері інформаційних технологій. Починаючи з 1998 року, Національна жандармерія відзначила пріоритетну діяльність у вирішенні проблем, пов'язаних з інноваційними технологіями, через створення відповідних структур та освітніх закладів, включаючи:

1. Відділ кіберзлочинів технічного обслуговування судових досліджень та документації (STRJD). Цей підрозділ моніторить Інтернет-мережу шляхом пошуку злочинів проти людей та майна, які пов'язані з нелегальним передачем даних в Інтернеті (веб-сайти, інтернет-ресурси, групи новин, мережі обміну, соціальні мережі та інше).

2. Відділ комп'ютерних та електронних технологій Інституту кримінальних розслідувань Національної жандармерії (IRCGN). Цей відділ розробляє методи, засоби та програмне забезпечення для автоматичного виявлення педофілів та інших порушників.

3. Окремі відділи збору інформації та проведення судових розслідувань (BDRIJ) та інші відомчі бригади. Додатковим органом у Франції, що займається запобіганням кіберзлочинності, є Національне агентство безпеки інформаційних систем (ANSII) – французьке агентство з кібербезпеки, яке співпрацює з державними спецслужбами. Діяльність цього агентства спрямована на втілення Французької національної стратегії цифрової безпеки, оголошеної

16 жовтня 2015 року. Ця стратегія, що впроваджується ANSSI, виникла внаслідок спільних зусиль між відомствами та спрямована на реагування на виклики цифрового століття. Цифровий перехід сприяє інноваціям та економічному розвитку, але несе й ризики для держави, бізнесу та громадян. Кіберзлочинність, шпигунство, пропаганда, саботаж та порушення приватності загрожують довірі та безпеці в цифровому середовищі. Основні пріоритети діяльності ANSSI включають захист та безпеку державних інформаційних систем та критичних інфраструктур, кібербезпеку, підвищення освіченості та навчання, сприяння розвитку бізнесу в цифровій сфері, забезпечення цифрової стратегічної автономії та стійкості кіберпростору.

Сучасні підходи до запобігання кіберзлочинності включають проведення спільних навчань, що є досить поширеним заходом. Під час цих навчань виявляють недоліки інфраструктури, розглядають варіанти атак та інцидентів, і пропонують найбільш ефективні методи реагування та координації.

Прикладом таких навчань є «Cyber Europe», які передбачають симуляцію значних інцидентів у сфері кібербезпеки, що наочно демонструють кібернетичні кризи. У цих вправах надається можливість аналізувати передові технічні інциденти в галузі кібербезпеки, а також розв’язувати складні ситуації щодо бізнес-контингенту та кризових ситуацій. Навчання «Cyber Europe» ілюструють різні сценарії, враховуючи реальні події, та були розроблені європейськими експертами з кібербезпеки [381].

Отже, для забезпечення кібербезпеки у Франції була створена відповідна нормативно-правова база, яка регулює функціонування органів, уповноважених забезпечувати кібербезпеку в країні. Захист кіберпростору та протидія кіберзлочинності є однією з головних пріоритетних мет для забезпечення національної безпеки Франції, і ця робота виконується не тільки поліцейськими органами (жандармерією), але й на рівні Міністерства оборони та спеціально утвореними установами [27].

Отже, виходячи з вищесказаного зазначимо, що у зарубіжних державах створена цілісна і розгалужена система державних органів і неурядових організацій, діяльність яких спрямована на запобіганні злочинності у сфері інформаційних технологій. Такі органи наділені власними повноваженнями щодо запобігання злочинності у сфері інформаційних технологій, в результаті

діяльності яких повністю реалізується система заходів запобігання даного виду злочинності [35].

Вважаємо, що досвід Франції щодо запобігання злочинності у сфері інформаційних технологій є актуальним для України. Особливо важливим є забезпечення ефективності роботи різних державних органів, кожен з яких має свої завдання, такі як розслідування, запобігання та облік осіб, які вчинили кримінальні правопорушення.

Необхідність впровадження ефективних заходів протидії сучасним загрозам інформаційній безпеці, зокрема кіберзагрозам, вимагає удосконалення форм і методів захисту інформації, критичної інформаційної інфраструктури та інформаційно-психологічної безпеки громадян. Цей підхід практикують у всіх європейських країнах. Україна, обравши курс на євроінтеграцію, повинна орієнтуватися на стратегію розвитку країн-учасниць Європейського Союзу в сфері інформації [224, с. 18]. При цьому, з урахуванням геополітичного положення України, основним орієнтиром повинні стати переважно країни Східної та Центральної Європи. Зокрема, останні є важливим прикладом успішної реалізації оптимальної моделі інформаційного суспільства. Вони досягли цього завдяки створенню високорозвиненої інфраструктури інформаційних технологій, що відзначається особливо високим рівнем доступу населення до цих технологій, випереджаючи інші країни світу за цими показниками. [225, с. 35].

На початку важливо відзначити, що Федеративна Республіка Німеччина, Угорська Республіка, Республіка Польща та Республіка Хорватія є членами Північноатлантичного Альянсу (НАТО) та Європейського Союзу (ЄС). У зв’язку з цим, на них поширюються стандарти цих міжнародних організацій, спрямовані на регулювання інформаційної політики та забезпечення інформаційної безпеки. Це включає стандарти НАТО з питань захисту інформації, які визначені в Документі CM (2002) 49 «Безпека в організації Північноатлантичного договору (НАТО)» [368], офіційна політика НАТО у сфері кіберзахисту [386], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту [387] й уточнена за результатами Варшавського саміту [388] тощо.

Не лише НАТО, але й Європейський союз активно ведуть політику забезпечення інформаційної безпеки. Сучасний Європейський Союз є об’єднанням високорозвинених країн, що мають значущий вплив на

міжнародні відносини та установлюють норми і стандарти поведінки держав у політичних, економічних, соціальних, інформаційних та інших сферах. В умовах сучасності важливим є комплексне вивчення підходу Європи до забезпечення інформаційної безпеки, зокрема з урахуванням євроінтеграційних стремлінь України.

В сучасній науковій літературі було розглянуто окремі аспекти інформаційної безпеки. Залежно від обговорюваних питань на тему європейської інформаційної безпеки можна класифікувати щонайменше за такими критеріями:

1. механізми та юридичне забезпечення захисту інформації у країнах Європи;
2. безпека е-управління та захист персональних даних у країнах ЄС;
3. загальна концепція політики інформаційної безпеки ЄС, ОБСЄ та НАТО;
4. сучасні інформаційні загрози та виклики для країн Європи й ін.;
5. інформаційна безпека України в контексті європейської інтеграції та інше.

Також важливо відзначити, що ще у 1991 році країни Європи розробили «Європейські критерії безпеки інформаційних технологій» [375]. Серед визначених завдань забезпечення інформаційної безпеки особливу увагу приділяється:

1. Захисту інформаційних ресурсів від несанкціонованого доступу для забезпечення конфіденційності.
2. Забезпеченню цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення.
3. Забезпеченню працездатності систем шляхом протидії загрозам відмови в обслуговуванні.

У 2001 році Європейська Комісія представила документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому описано сучасний підхід ЄС до проблеми інформаційної безпеки. Документ визначає основні напрямки європейської політики інформаційної безпеки:

1. Підвищення обізнаності користувачів щодо можливих загроз під час використання комунікаційних мереж.
2. Створення європейської системи попередження та інформування про нові загрози.
3. Забезпечення технологічної підтримки.

4. Підтримка ринково орієнтованої стандартизації та сертифікації.

5. Правове забезпечення з пріоритетами у захисті персональних даних, регулюванні телекомунікаційних послуг та протидії кіберзлочинності.

6. Зміцнення інформаційної безпеки на державному рівні через впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання електронних підписів країнами-членами під час надання державних онлайн послуг.

7. Розвиток міжнародного співробітництва з питань інформаційної безпеки.

Дії, які порушують безпеку інформаційних мереж та систем, можна умовно поділити на такі категорії: перехоплення електронної комунікації, копіювання або зміна даних; несанкціонований доступ до комп'ютера або комп'ютерних мереж; атаки, спрямовані на знищення мереж, такі як атаки на доменні імена, перевантаження мережі штучними повідомленнями та атаки на маршрутизацію; використання шкідливого програмного забезпечення; фальсифікація веб-сайтів; безпекові інциденти, спричинені непередбачуваними та неумисними подіями, такими як природні катастрофи, збої апаратного та програмного забезпечення та помилки людини.

Історично 10 березня 2004 року була заснована Європейська агенція з мережевої та інформаційної безпеки (ENISA), яка спрямована на підвищення потенціалу європейської спільноти та країн-членів у попередженні та реагуванні на проблеми, пов'язані з інформаційною безпекою.

Основні напрями діяльності Агентства включають:

– Надання консультацій та допомоги Комісії та країнам-членам у сфері інформаційної безпеки.

– Збір та аналіз даних про безпекові інциденти в Європі та ризики, пов'язані з ними.

– Розробка методів оцінки та управління ризиками для підвищення готовності ЄС реагувати на загрози інформаційній безпеці.

– Підвищення обізнаності та розвиток співробітництва між різними учасниками у сфері інформаційної безпеки, зокрема, шляхом сприяння взаємодії між державним та приватним секторами.

Агентство також надає допомогу Європейській Комісії у попередній технічній роботі для оновлення та вдосконалення

європейського законодавства в галузі мережевої та інформаційної безпеки.

У своїй діяльності Агенція керується щорічними робочими планами та програмами, які включають у себе перерахування основних пріоритетів, цілей та запланованих заходів для виконання намічених завдань. Наприклад, у робочій програмі Агенції на 2010 рік визначено стратегічні пріоритети, такі як підвищення опору європейських електронних мереж зовнішнім впливам; сприяння розвитку співробітництва між країнами-членами у сфері інформаційної безпеки; виявлення нових ризиків в сфері інформаційної безпеки та встановлення взаємної довіри між зацікавленими особами для ефективного реагування на ці ризики [130].

Однак сучасні терористи активно використовують Інтернет для поширення своєї пропаганди на веб-сайтах, форумах та у відеороликах, перш за все, щоб повідомляти про свої успіхи та залучати прихильників. В історії Інтернету були випадки руйнування стартових сторінок веб-сайтів з політичними метами (зокрема, військових чи урядових). Також відомі кібератаки, спрямовані на перевантаження серверів і блокування доступу до них. Зазвичай це результат дій ентузіастів або груп фанатиків і наразі не спричинили значних матеріальних, фінансових або людських втрат.

Однією з наймасштабніших інформаційних атак на Інтернет за його історію була атака мережевого злочинця Хелкерн, яка сталася 26 січня 2003 року та тривала два дні. Вплив Хелкерна на світові інформаційні ресурси був визнаний експертами з комп'ютерної безпеки безпрецедентним випадком за швидкістю поширення та розмірами спричиненої та потенційної шкоди – оцінюється більш ніж в 10 мільярдів доларів. У результаті було інфіковано 80 тисяч веб-серверів, а Інтернет уповільнив свою роботу у всьому світі в середньому на 25 %. Аналітики вважають, що Хелкерн став «важливим кроком у створенні інформаційної зброї», оскільки жодному вірусу до цього не вдавалося настільки ефективно заважати обміну інтернет-трафіком.

Аналіз відомих кібератак свідчить про те, що міжнародні терористичні та екстремістські організації, такі як Хамаз і Аль-Каїда, а також національні сепаратистські рухи, вже освоїли і використовують інформаційно-комунікативні технології. Проте на сьогодні терористи надалі надають перевагу фізичному ураженню реальних осіб реальними бомбами, щоб залякати населення через

ЗМІ, ніж вчиняти віртуальні атаки через Інтернет. На думку експертів, проблема полягає не стільки у кібертероризмі, скільки у кіберзлочинності та, можливо, навіть у кібервійні.

Окремі зловживання засобами інформаційно-комунікативних технологій спонукають до запровадження превентивних заходів для їх подолання. Наприклад, після атаки на банківські та урядові сервери Естонії у 2007 році, країна вступила до НАТО та створила два центри кібероборони: один у Брюсселі та інший у Таллінні.

Сполучені Штати Америки, які створили широку мережу телекомунікаційного шпигунства (відому як Echelon) під час «холодної війни», проголосили про запуск плану, який спрямований на забезпечення їхнього лідерства в кіберпросторі. Цей план є результатом проєкту «Манхеттен» (який привів до створення першої атомної бомби) і включає декілька завдань: моніторинг світового Інтернет-трафіку та запитів у пошукових системах; створення «троянських програм», які дозволяють отримати контроль над будь-яким комп'ютером; а також використання Інтернету (та його користувачів) для випробування сценаріїв атак та оборони, а також для навчання військових кіберпідрозділів. Отже, цей проект має двоїстий характер. З одного боку, він є одним із засобів превентивної оборони у боротьбі з кібертероризмом. З іншого боку, він є одним із засобів реалізації геополітичних амбіцій США.

У січні 2003 року офіційні представники США заявили, що Міністерство оборони може провести інформаційну війну у разі інформаційного нападу на країну. На початку лютого того ж року офіційні особи з Адміністрації Президента США повідомили, що Дж. Буш підписав секретну директиву. Згідно з нею уряд має вперше розробити національне керівництво, яке визначатиме умови, за яких Сполучені Штати здійснюватимуть кібератаки на комп'ютерні мережі своїх супротивників, а також правила проникнення в іноземні комп'ютерні системи та порушення їх нормальної роботи [182].

Безсумнівно, активне використання інформаційно-комунікаційних технологій призвело до появи нових загроз для міжнародної безпеки. Це поставило перед міжнародною спільнотою серйозне завдання – розробити міжнародно-правові заходи для запобігання кібер-злочинності, кібертероризму та запобігання кібервійнам. Ускладнює ситуацію той факт, що до сьогодні не існує загальноприйнятого визначення «інформаційної зброї». Відомо, що цей термін став

вживатися в американських військових колах у 1991 році після закінчення війни у Персидській затоці.

Ускладнює питання щодо визначення та обставин те, що інформаційні технології в основному використовуються як технології невійськового або подвійного призначення. Інформаційно-комунікаційні технології, які можуть бути використані для військових операцій, в основному починають використовуватися у цивільному секторі. Характерними ознаками інформаційної зброї є універсальність, радикальність застосування та доступність. Впровадження цієї зброї не вимагає значних фінансових витрат, що робить інформаційну війну економічно доступним і, отже, небезпечним засобом військової боротьби, яка часто має характер мирної діяльності. Важко визначити державу, що здійснила інформаційну атаку одночасно. Використання цієї зброї може відбуватися приховано, без оголошення війни і не вимагає видимої підготовки. Жертва може навіть не усвідомлювати, що перебуває під впливом інформації.

Важливо пам’ятати про потенційні загрози правам та свободам громадян у контексті застосування інформаційної зброї. Перш за все, це може вразити основні цінності демократії: право на свободу поширення та доступ до інформації, конфіденційність особистої інформації та інші. Крім того, засоби інформаційного впливу можуть використовуватися як психотропна зброя. Очевидно, що потрібно забезпечити міжнародну інформаційну безпеку за допомогою міжнародно-правових інструментів [182] .

Отже, очевидно, що потрібно забезпечити міжнародну інформаційну безпеку шляхом міжнародно-правових засобів. Міжнародне право лише розпочинає процес її регулювання.

Загалом, важливо відзначити, що прихованість розробки засобів для проведення інформаційних воєн, притаманність ІКТ до технологій подвійного призначення та їх поєднання зі звичайними засобами ведення бойових дій, практично неконтрольоване створення, використання і недостатньо суворе регулювання кіберпростору може призвести до катастрофічних наслідків для людської цивілізації. Цьому може запобігти лише міжнародна співпраця всіх країн у сфері інформаційної безпеки. Заснована на збалансованих міжнародних нормативно-правових актах, які враховують особливості національного законодавства та вимагають політичної волі, ця співпраця

спроможна створити ефективну систему міжнародної інформаційної безпеки.

4.2. Міжнародно-правові стандарти запобігання злочинності у сфері інформаційних технологій

Незважаючи на те, що злочинність у сфері інформаційних технологій з'явилися нещодавно, вона стали серйозною загрозою сучасному світовому суспільству. Протягом кожного року це явище набуває більшого розповсюдження та складності як вид злочинності, що вимагає розробки відповідної правової теорії та методологічного інструментарію, особливо у галузі кримінального права та кримінології.

Більшість кримінальних правопорушень у цій сфері, як було зазначено раніше, не обмежуються лише територією конкретної країни чи віртуальним простором. Ці кримінальні правопорушення можуть мати глобальний, міждержавний або навіть міжнародний характер. Це вимагає міжнародного співробітництва, оскільки однією з основних проблем для правоохоронних органів під час розслідування кримінальних правопорушень у цій сфері є складність визначення особи злочинця, територіального розташування його країни та применшення відповідних правових норм [70].

Таким чином, стає очевидною необхідність забезпечення міжнародної інформаційної безпеки за допомогою міжнародно-правових засобів. Міжнародне право лише розпочинає регулювати цю сферу.

У своєму звіті від 10 травня 1999 року Генеральний секретар ООН визнавав існування проблеми в галузі міжнародної інформаційної безпеки (далі – МІБ). Резолюція 53/70 поклала початок обговоренню потреби у створенні нового міжнародно-правового режиму для регулювання сфери інформаційного простору, ІКТ та методів її використання. У 1999 році в Женеві відбувся міжнародний семінар з питань міжнародної інформаційної безпеки, в якому взяли участь представники понад 50 країн. Його результатом стало підтвердження актуальності проблеми інформаційної безпеки та актуальності її обговорення на міжнародному рівні. На 54 сесії Генеральної Асамблеї ООН був представлений проект резолюції «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки». Важливим аспектом було висловлення турботи щодо можливого

неправомірного використання засобів ІКТ «з цілями, що несумісні із завданнями забезпечення міжнародної стабільності та безпеки», що може негативно вплинути на безпеку держав як у громадянській, так і у військовій сферах. З урахуванням необхідності запобігання «неправомірному використанню або використанню інформаційних ресурсів чи технологій у кримінально протиправних або терористичних цілях», Генеральна Асамблея підняла питання про «доцільність розробки міжнародних принципів, спрямованих на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем та сприяння боротьбі з інформаційним тероризмом і криміналом».

У резолюції, прийнятій консенсусом 29 листопада 2001 року (документ A/RES/56/19), схвалена ідея створення в 2004 році спеціальної Групи урядових експертів держав-членів ООН для проведення усебічного дослідження проблеми міжнародної інформаційної безпеки. Мандат Групи включає в себе аналіз існуючих та потенційних загроз у сфері інформаційної безпеки і можливість спільних заходів для їх запобігання. Також передбачено вивчення міжнародних концепцій, спрямованих на посилення безпеки глобальних інформаційних та телекомунікаційних систем. Згідно з резолюцією, результатом роботи Групи буде представлення Генсекретарем ООН звіту Генеральній Асамблеї у 2005 році, що відображатиме результати цього дослідження.

У наступному періоді здійснюється виконання рішення міжнародної спільноти про необхідність глибокого аналізу питань міжнародної інформаційної безпеки. Приймаються резолюції, що розширюють положення попередніх та підтверджують недопустимість негативного впливу на інфраструктуру держав за допомогою інформаційно-телекомунікаційних технологій. Наприклад, 23 січня 2002 року Генеральна Асамблея ООН прийняла резолюцію, в якій обговорювалася боротьба з кримінально протиправним використанням інформаційних технологій. Документ наголошував на необхідності міжнародної співпраці та взаємодії між державами та приватним сектором у запобіганні кримінально протиправного використання інформаційно-комп’ютерних технологій. Також він акцентував увагу на важливості сприяння доступу до цих технологій країнам, що розвиваються, оскільки розбіжності в доступі та використанні таких технологій можуть негативно вплинути на ефективність боротьби зі злочинністю у цій сфері.

У 2002 році під час Загальноєвропейської конференції в Бухаресті була ухвалена декларація, яка встановила принцип посилення довіри та безпеки під час використання інформаційно-комп'ютерних технологій. Вона передбачала створення «глобальної культури кібербезпеки», сприяючи запровадженню запобіжних заходів та отриманню підтримки від усього співтовариства, за умови збереження свободи обміну інформацією. Країни погодилися, що важливо «передбачати неправомірне використання інформаційних ресурсів та технологій у протиправних або терористичних цілях» і зміцнювати міжнародну співпрацю у цьому напрямі.

На Всесвітньому саміті з питань інформаційного суспільства, який відбувся у Женеві у 2003 році та у Тунісі у 2005 році, було обговорено регулювання інформаційного простору та створення інформаційного суспільства з метою «створення інформаційного суспільства, орієнтованого на інтереси людей», яке було б відкритим для всіх та спрямоване на розвиток суспільства. Це суспільство мало б забезпечувати можливість кожній особі створювати, мати доступ до, використовувати та обмінюватися інформацією та знаннями, щоб окремі особи, громади та народи мали можливість повністю реалізувати свій потенціал для сталого розвитку та підвищення якості життя [138].

За підсумками Женевської фази Всесвітнього саміту найвищого рівня, що відбулася 12 грудня 2003 р., була прийнята Декларація принципів «Розбудова інформаційного суспільства є глобальним завданням нового тисячоліття», яка стала для нового життя інформаційного суспільства [89].

На цьому етапі було затверджено План дій, який становить основу для руху до інформаційного суспільства на рівнях країни, регіону та міжнародного співтовариства. Установлені в цьому плані часові рамки сприятимуть втіленню концепції відкритого та справедливого інформаційного суспільства для всіх [114].

У Токійській декларації, яку ухвалили представники 47 країн, 22 міжнародних та 116 неурядових організацій, а також представники 54 приватних компаній під час зустрічі з 13 по 15 січня 2003 року, були визначені «пріоритетні напрямки» у сфері інформаційно-комп'ютерних технологій. Важливим аспектом серед них є забезпечення безпеки інформаційних технологій та засобів. Визнаючи принцип справедливого, рівного та адекватного доступу до інформаційних комп'ютерних технологій для всіх країн, особлива увага мала бути

зосереджена на загрозі потенційного військового використання цих технологій. У цьому контексті вперше була висловлена думка, що ефективне забезпечення інформаційної безпеки може бути досягнуте не лише технологічно, але й за умови зусиль у сфері правового регулювання та розроблення відповідних національних політик [182].

Загальна думка з вищезазначеного випливає на те, що боротьба з кіберзлочинністю та потреба у міжнародному співробітництві в цьому контексті вимагає створення міжнародних процедур надання допомоги під час розслідування таких кримінальних правопорушень та утворення координаційних органів в межах міжнародних правоохоронних установ, таких як ООН, Інтерпол, Рада Європи та інші.

Низка міжнародних документів підкреслює, що злочинність у сфері інформаційних технологій на сьогодні становить загрозу не лише національній безпеці окремих країн, але й загрожує безпеці людства та міжнародному порядку. Стурбованість міжнародного співтовариства щодо поширення злочинності у сфері інформаційних технологій виявилася у таких міждержавних угодах як Бангкокська декларація з попередження злочинності та кримінального правосуддя (2005 р.), Бухарестська декларація про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.), Всесвітній саміт з інформаційного суспільства та Конвенції Ради Європи «Про кіберзлочинність» (2001 р.). У цих документах обговорюється спільне протистояння кіберзлочинам через прийняття ефективного законодавства, яке не порушує ні внутрішні закони окремої країни, ні умови міжнародних угод, у які ця країна є стороною [270].

Відповідно до рішень резолюцій Генеральної Асамблеї ООН 56/183 від 21 грудня 2001 року та 57/238 від 20 грудня 2002 року у Женеві з 10 по 12 грудня 2003 року відбувся перший етап Всесвітньої зустрічі на найвищому рівні з питань інформаційного суспільства. Другий етап був запланований на 16–18 листопада 2005 року у Тунісі. Ця зустріч стала першим міжнародним форумом, де обговорення питань, пов’язаних з глобальними процесами інформатизації, піднято на найвищий політичний рівень, і відбулося в широкому геополітичному масштабі у взаємодії з представниками бізнес-середовища та громадського суспільства. На саміті були присутніми понад 11 тисяч осіб з 176 країн світу, включаючи представників міжнародних

організацій. Питання інформаційної безпеки займало центральне місце у міжнародній увазі під час цієї зустрічі [338].

На заключний акорд першого етапу зустрічі вплинуло ухвалення двох документів: Декларації принципів та Плану дій. Ці документи охоплюють різноманітні аспекти формування глобального інформаційного суспільства і основні напрямки міжнародної співпраці в цій сфері. Серед них важливі аспекти включають розробку та розширення інформаційно-комунікаційної інфраструктури, забезпечення безпеки при використанні інформаційних комп'ютерних технологій, забезпечення доступу до інформації, інфраструктури та послуг, що базуються на цих технологіях [204].

У Декларації принципів, особливо в розділі «Зміцнення довіри та безпеки при використанні інформаційних комп'ютерних технологій», відзначається, що підвищення рівня довіри, включаючи безпеку інформації та мереж, є важливою передумовою становлення інформаційного суспільства.

Важливі аспекти протистояння інформаційній злочинності були зафіксовані в резолюції 58 Генеральної Асамблеї ООН від 30 січня 2004 року «Створення глобальної культури кібербезпеки та захисту найважливіших інформаційних структур». Серед них основними є формулювання переліку заходів для захисту найважливіших інформаційних інфраструктур. Це включає як міжнародні, так і національні заходи, які є ключовими елементами для побудови глобальної системи запобігання спробам використання інформаційних комп'ютерних технологій для цілей, що не відповідають основним принципам міжнародного права та загрозам безпеці держави, суспільства та особистості.

Треба відзначити, що криміналізація дій, які утворюють злочинність у сфері інформаційних технологій, є окремою науковою та практичною проблемою, яка може бути вирішена лише через розробку універсальної концепції кіберзлочинності та уніфікацію норм міжнародного права.

Отже, під час запобігання злочинності у сфері інформаційних технологій відсутній консенсус та єдність в міжнародному правовому вимірі. Це невід'ємно призводить до зменшення ефективності контролю та сприяє виникненню конфліктів і прогалин. В той самий час швидкі технологічні просування відбуваються настільки стрімко, що ця проблема у майбутньому стане ще більш актуальною.

15 січня 2015 року Генеральна Асамблея прийняла резолюцію A/RES/69/204 щодо використання інформаційно-комунікаційних технологій (ІКТ) для сприяння розвитку. У цьому документі було виділено позитивний вплив на збільшення доступності ІКТ та фінансування, зокрема розширення доступу до Інтернету, розвитку мобільного зв'язку та швидкого поширення комунікаційних зв'язків. Проте в той же час викликає занепокоєння значна різниця між розвиненими та країнами, які розвиваються, у покритті широкосмуговим зв'язком, нерівній можливості доступу до ІКТ з позицій гендерного аспекту та негативний вплив на інвестиційну діяльність [274].

У резолюції A/RES/70/237 від 2015 року Генеральна Асамблея закликала країни-члени сприяти міжнародному обговоренню наявних та можливих загроз інформаційній безпеці, а також розглядати можливі стратегії в цій сфері, за необхідності, для забезпечення вільного потоку інформації. Також наголошувалося на необхідності продовжувати аналізу відповідних міжнародних концепцій з метою посилення безпеки глобальних інформаційних і телекомунікаційних систем [273].

Узагальнюючи, слід відзначити, що Генеральна Асамблея ООН виступає важливим консультативним органом ООН, що обговорює актуальні питання, що стосуються інтересів країн-членів та інших держав, зокрема, боротьбу зі злочинністю у сфері інформаційних технологій. Під її патронатом прийнято низку законопроєктів, що охоплюють аспекти: регулювання інформаційного простору, захисту інформаційної інфраструктури, безпеки користувачів Інтернет-сервісів, культури кібербезпеки та міжнародної співпраці у боротьбі з кіберзлочинністю, зокрема, обмін інформацією, професійна підготовка правоохоронців, забезпечення конфіденційності, цілісності та доступності даних комп'ютерних систем. Генеральна Асамблея є ініціатором створення спеціалізованих груп експертів для вивчення аспектів боротьби з кіберзлочинністю та спеціалізованих організацій ООН, які координують запобігання злочинності у сфері інформаційних технологій (Управління ООН з наркотиків і злочинності, Конференція ООН з торгівлі і розвитку, Міжнародний союз електрозв'язку, Організація Об'єднаних Націй з питань освіти, науки і культури, Конференція ООН з торгівлі і розвитку тощо). При аналізі законодавства України з питань інформаційної безпеки можна зробити висновок про визнання країною проблем, що пов'язані з інформаційною безпекою.

Певною мірою визнання існування проблем пов'язаних з інформаційною безпекою є прийняття юридичних норм, що регулюють суспільні відносини у даній сфері. Наприклад:

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Закон України «Про державну таємницю»;

– Закон України «Про основи національної безпеки України»;

– Указ Президента України № 891 від 24.09.2001 року «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних»;

– Указ Президента України № 1229 від 27.09.1999 року «Про Положення про технічний захист інформації в Україні» тощо.

Знову таки, певною мірою визнання того факту, що у даній сфері суспільних відносин можуть траплятися кримінальні прояви є прийняття нормативних документів, котрі встановлюють відповідальність за кримінальні правопорушення, вчинені в інформаційній сфері. Прикладом можуть бути:

– Розділ 16 Кримінального Кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»;

– визначення «технологічного тероризму» у Законі України «Про боротьбу з тероризмом», де говориться про кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням засобів електромагнітної дії, комп'ютерних систем та телекомунікаційних мереж.

Але хотілось більш детально звернути увагу на положення Указу Президента України «Про Доктрину інформаційної безпеки України» № 514/2009 від 08.07.2009 р., які визначають позицію нашої держави, саме у сфері міжнародній інформаційній безпеці. Так, напрямами діяльності у сфері зовнішньої політики, зокрема, є:

– якісне вдосконалення інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном за пріоритетами стратегічного партнерства та економічної доцільності;

– організаційно-технічне, інформаційне та ресурсне сприяння держави вітчизняним засобам масової інформації, які мають формувати у світовому інформаційному просторі позитивний імідж України;

– посилення інформаційно-просвітницької діяльності серед населення щодо забезпечення національної безпеки України за умов повноправного партнерства з країнами-членами ЄС та Північноатлантичного альянсу;

– інтеграція в міжнародні інформаційно-телекомунікаційні структури та організації на засадах рівноправності, економічної доцільності та збереження інформаційного суверенітету;

– гарантування своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації [258].

У звіті Національної поліції України за 2021 рік є розділ, який присвячений роботі кіберполіції, її завданням було виявлення осіб, які вчиниди кримінальні правопорушення в інформаційній сфері. Зазначається, що в 2021 році було зафіксовано майже вдвічі більше кримінальних правопорушень, вчинених з використанням високих інформаційних технологій. Зокрема, спостерігалося майже півторазове збільшення кримінальних правопорушень у банківській сфері та третина збільшення в сфері комп'ютерних систем.

Кіберполіцейські у 2021 році ініціювали проведення 9 міжнародних поліцейських операцій і взяли участь у 8 таких заходах за запрошенням іноземних колег. У звіті наведено приклади встановлення осіб, підозрюваних у створенні вірусу «EMOTET», які завдали значних збитків потерпілим. Також вказано на встановлення осіб, які застосували шкідливе програмне забезпечення «Ransomware» та завдали збитків компаніям Республіки Корея та США.

Крім того, кіберполіція спрямовує зусилля на попередження та профілактику кіберзлочинів, підтримуючи прямий зв'язок з громадянами та реагуючи на протизаконні дії в сфері кіберпростору. У 2021 році кіберполіція отримала понад 190 тис. звернень від громадян, більшість з яких надійшли до call-центру та через електронні запити.

У звіті Національної поліції України про результати роботи у 2021 році було зафіксовано значне зростання кількості комп'ютерних злочинців порівняно з попереднім роком. У 2020 році виявлено 5240 комп'ютерних злочинців, у той час як у 2021 році ця кількість зросла до 10020. Зокрема, у 2020 році найбільша кількість злочинів була пов'язана з банківською сферою (2110), онлайн шахрайствами (1355) та сферою комп'ютерних систем (1461). У 2021 році ці показники також значно зросли: у банківській сфері було зафіксовано

3049 кримінальних правопорушень, пов'язаних з онлайн шахрайствами – 1928 та у сфері комп'ютерних систем – 1981 [132].

Слідча, експертна і судова практика українських правоохоронних органів, які займаються запобіганням кіберзлочинності, також свідчить про постійний зріст кількості кримінальних порушень, які вчиняються за допомогою електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, включаючи тяжкі та менш тяжкі правопорушення, в Україні. Наприклад, якщо у 2016 році в Україні зареєстровано лише 818 таких кримінальних правопорушень, то вже в 2017 році кількість зареєстрованих кримінальних порушень зросла до понад 2514, а станом на початок серпня 2022 року вже зафіксовано аж 1945 таких кримінальних правопорушень [124].

Судова статистика свідчить про стрімке зростання комп'ютерних кримінальних правопорушень, вчинених у 2022 році в Україні та світі. Крім цього, багато розслідувань кримінальних правопорушень у сфері інформаційних технологій, здійснених органами України, були призупинені через потребу проведення процесуальних дій у рамках міжнародного співробітництва. Це означає, що такі такі протиправні діяння можуть розслідуватись протягом кількох років.

До того ж, очевидно, що наявні дані в органах правосуддя не повністю відображають сучасний рівень злочинності в галузі інформаційних технологій в Україні. З цієї причини, як правильно вказує Н. М. Ахтирська, потрібні суттєві зміни у законах та інших нормативно-правових актах, які визначають відповідальність за вчинення кримінальних правопорушень з використанням комп'ютерних технологій. Також необхідно удосконалювати процесуальне законодавство щодо збору доказів, розширювати міжнародне співробітництво під час кримінального розслідування та надавати належну підготовку кадрів для розслідування кіберзлочинів [14, с. 5].

Оскільки усвідомлено, що в Україні недостатньо проводиться спеціалізована професійна підготовка у галузі кібербезпеки для представників органів правосуддя, адвокатів та кіберполіції, це пов'язано з тим, що сучасні прокурори, судді, представники кіберполіції та адвокатури фактично не мають достатніх правових, технічних, кримінологічних, криміналістичних та експертних знань у цьому швидко розвиваючому сегменті електронного цивілізаційного прогресу [26].

Враховуючи, що в Україні наразі недостатньо звертається увага на базову професійну підготовку для запобігання комп'ютерній злочинності, вважаємо належним установити систематичну підготовку відповідних спеціалістів у закладах вищої освіти.

Ці нововведення також відображені в Угоді про асоціацію України з Європейським Союзом, де чітко вказано, що протистояння кіберзлочинності є ключовим елементом політики безпеки [317].

Для досягнення цілей щодо кібербезпеки на загальнодержавному рівні слід прийняти комплекс заходів, які охоплюють законодавчі, організаційні, кадрові, освітні, правові та ресурсні аспекти. Важливість цих питань віднайшла відображення у Стратегії національної безпеки України, яка вказує на необхідність підвищення спроможності правоохоронних органів у запобіганні, протидії та розслідуванні кримінальних правопорушень у сфері інформаційної безпеки, створення системи підготовки фахівців у галузі кібербезпеки, кіберкримінології, кіберкриміналістики та кіберекспертології, а також встановлення міжнародного співробітництва в сфері забезпечення кібербезпеки [256].

Захист громадян від зазначених кіберзлочинів є важливим завданням для кіберполіції України та інших органів держави.

Також слід пам'ятати про особисту інформаційну безпеку та дотримуватися основних принципів:

– Використовувати ліцензійне програмне забезпечення.

– Утримувати персональні дані, дані та паролі до банківських карток та систем від доступу сторонніх осіб.

– Уникати завантаження та відкриття підозрілих комп'ютерних файлів.

– Перевіряти інформацію, особливо банківську, лише на офіційних веб-сайтах або за офіційними номерами телефону.

– Уникати відвідування та введення особистих даних на сумнівних веб-сайтах.

– Бути обережними щодо повідомлень у месенджерах або СМС щодо сумнівних акцій та виграшів.

– Використовувати антивірусні програми.

– Використовувати складні та різнорідні паролі та уникати їх збереження на телефоні чи комп'ютері.

– Уникати зберігання особистої інформації небажаного характеру на телефонах та комп'ютерах та інші схожі заходи.

Дотримання цих правил сприятиме уникненню або мінімізації ризику стати об'єктом уваги кіберзлочинців. Тому вважаємо, що особливу увагу сьогодні потребують питання, пов'язані з розвитком грід- та блокчейн-технологій, впровадженням криптовалюти, перспективами ефективного використання Всесвітньої мережі – Інтернету, соціальних мереж, комп'ютерних ігор, запровадженням процедури біометричних паспортів (ID-карток), створенням новаторських стартапів, формуванням банків віртуальної власності, перспективами подальшого розвитку Інтернету речей, електронної комерції, обов'язкового забезпечення конституційного права людини на інформацію та гарантуванням надійної кібербезпеки та реальних механізмів компенсації завданої шкоди в кіберсфері. [6, с. 16–17].

Викладене вище вказує на те, що всі ці складні аспекти (загрози, ризики та небезпеки в кіберпросторі) потребують належного правового, освітнього та наукового забезпечення для глибокого вивчення особливостей комп'ютерних злочинців як об'єктів кримінологічного аналізу. Саме ці суттєві аспекти є об'єктом даного кримінологічного дослідження. Аналізуючи стан та тенденції розвитку інформаційно-комунікаційних технологій в Україні і світі, ми приходимо до висновку про необхідність удосконалення діючого законодавства та розширення організаційно-технічного та ресурсного забезпечення у сфері освітньої та наукової діяльності з протидії та запобігання комп'ютерній злочинності в умовах формування четвертої промислової революції, Індустрії 4.0 та розвитку суспільства знань [6, с. 16–17].

Слід відзначити, що кіберзлочинність і кібертероризм, що є складовою кіберзлочинності, представляють сучасні та надзвичайно небезпечні загрози для ефективного розвитку суспільства, держави та цивілізації. Отже, важливо акцентувати увагу на розширенні мережі кримінологічних наукових досліджень, що стосуються комп'ютерних злочинів, вчинених комп'ютерними злочинцями.

Вищезазначене вказує на пріоритетні напрямки для впровадження на даному етапі розвитку електронної цивілізації. Особливу вагу мають такі наукові аспекти, як визначення поняття та сутності фізичної особи комп'ютерного злочинця, аналіз структури кримінологічних характеристик особи комп'ютерного злочинця, удосконалення правових і наукових засад дослідження кримінологічного портрету комп'ютерного злочинця, створення кри-

мінологічної типології особи комп'ютерного злочинця, удосконалення структури та основних елементів систематизації та класифікації комп'ютерних злочинців, проведення міжнародного та вітчизняного порівняльного аналізу кримінологічної класифікації та характеристики комп'ютерних злочинців, вдосконалення поняття, сутності та загальної характеристики кримінологічних засобів дослідження комп'ютерного злочинця, визначення можливостей використання новітніх засобів, методів та технологій для кримінологічного дослідження особи комп'ютерного злочинця, виявлення причин та умов розвитку комп'ютерної кіберзлочинності, а також розроблення праксеологічних заходів щодо її запобігання та протидії, а також формування теоретичних основ нової галузі знань – соціально комунікаційної електронної інженерії особистості комп'ютерного злочинця, створення концептуальних основ правового, кримінологічного, освітнього та праксеологічного забезпечення дослідження особи комп'ютерного злочинця як об'єкта кримінологічного дослідження; удосконалення законодавчого регулювання правових відносин у сфері соціально-комунікаційної індустрії з метою запобігання комп'ютерним злочинам у кіберпросторі; розроблення нових засобів, методів, програм і технологій у сфері комп'ютерної діагностики особи комп'ютерного злочинця; формування стратегій, тактик і мистецтва використання даних про особу комп'ютерного злочинця для запобігання злочинності в кіберпросторі; розробка системи пріоритетних напрямків запобігання комп'ютерній злочинності у наземному та космічному просторі на основі вивчення даних про особу комп'ютерного злочинця; вивчення можливостей використання сучасних засобів ідентифікації особи комп'ютерного злочинця для запобігання кримінальних правопорушень у кіберпросторі; розроблення концептуальних засад запобігання вчиненню комп'ютерних злочинів електронним інтелектом проти людини, суспільства та держави; аналіз стану та тенденцій криміногенного впливу комп'ютерної злочинності у галузі соціально-комунікаційної індустрії на основі цивілізаційного розвитку суспільства [6, с. 344].

Цифрові технології стали неодмінною частиною нашого щоденного життя і, як ніщо інше, сприяють процесу глобалізації. У той же час протиправна діяльність також користується перевагами інформаційних технологій, не маючи меж. Це підкреслює актуальність міжнародного рівня боротьби з кіберзлочинністю, що

передбачає впровадження в національні правові системи спільних правових заходів.

Після ратифікації 07.09.2005 р. Конвенції про кіберзлочинність (надалі – Конвенція) Україна взяла на себе зобов'язання впровадити широкий спектр матеріально-правових та процесуальних заходів для боротьби з кіберзлочинністю. Довгий час багато з механізмів, передбачених Конвенцією, не були належним чином реалізовані в національному процесуальному законодавстві, залишаючись предметом наукового аналізу та компенсуючись у практичній діяльності через існуючі процесуальні процедури. Наприклад, запити щодо термінового збереження комп'ютерних даних реалізуються через тимчасовий доступ до них [325].

Індикатором можливості в майбутньому у певній мірі виправити описану ситуацію є зацікавленість законодавця, яка відображена у проєкті Закону «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення з метою підвищення ефективності протидії кібератакам» № 4003 від 01.09.2020 р. (далі – проєкт № 4003). Цей проєкт має важливий науковий обґрунтований базис, спрямований на аналіз та висловлення зауважень і пропозицій щодо вдосконалення процесуальних механізмів.

Мета цього законопроєкту полягає в адаптації «положень Конвенції про кіберзлочинність у кримінальне процесуальне законодавство України та підвищенні ефективності боротьби з кібератаками» [230].

Мова йде про наступні стандартні механізми Конвенції:

а) утримання комп'ютерних даних у невідкладних випадках (ст. 16 Конвенції);

б) обмежене розкриття даних щодо руху інформації (ст. 17 Конвенції); в) розширення обсягу обшуку у комп'ютерних даних (пп. 2,4 ст. 19 Конвенції).

Пропонується впровадити ці механізми в кримінальному процесуальному законі через наступні положення:

1. новий захід забезпечення кримінального провадження – утримання інформації в невідкладних випадках (зміни до ст. 131, 303, додаток нової Глави 151), а також його процесуальні особливості:

а) право делегувати виконання (зміни до ст. 36, 40, 41);

б) можливе електронне ухвалення рішення про його застосування (зміни до ст. 110); в) право оскарження рішення про його застосування (зміни до ст. 303);

2. адаптація існуючого заходу забезпечення – тимчасовий доступ до речей та документів для отримання доступу до невідкладно збереженої інформації (зміни до ст. 159, 162, 303, додаток нових статей 1641, 1651);

3. право під час проведення обшуку:

а) отримувати віртуальний доступ до цифрового пристрою, фізичне розташування якого відрізняється від об'єкта обшуку;

б) подолання логічної системи захисту цифрового пристрою;

в) отримувати інформацію про цифрові особливості пристроїв (зміни до ст. 236).

Важливо розглядати ці положення проєкту № 4003 в такій послідовності.

Термінове збереження інформації. Викладені у проєкті № 4003 положення про термінове збереження інформації викликають низку зауважень у контексті як конвенційних ідей, так і національного законодавства. Розуміння нового заходу забезпечення кримінального провадження як невідкладного фіксування та подальшого зберігання інформації в електронній (цифровій) формі, яка має значення для встановлення обставин у кримінальному провадженні (абз. 2 ч. 1 ст. 166^1 КПК у редакції проєкту № 4003):

1) не виключає можливості поширення його дії на інформацію, яку буде отримано у майбутньому (натомість конвенційний захід призначений виключно для інформації, яка на момент застосування процесуальної дії вже зберігається в особи, на чому неодноразово наголошували міжнародні експерти [134];

2) викликає термінологічні зауваження:

а) замість терміна «інформація» радше вживати згаданий у Конвенції «дані», більш коректний із технічної точки зору;

б) поєднання прикметників «електронний» та «цифровий» для характеристики форми інформації недоцільне: перший характеризує носії даних, другий – власне дані або інформацію;

в) невиправданим видається вживання терміна «фіксування», який асоціюється з відповідним процесуальним інститутом (глава 5 розділу І Кримінального процесуального кодексу України (далі – КПК). Замість цього можна запропонувати таке формулювання: «Термінове збереження даних полягає у підтриманні їхньої

цілісності, тобто недопущенні дій, що можуть привести до втрати або зміни цифрових даних».

Перший абзац вищезгаданої частини статті не розглядає всі можливі недоліки. Відзначається, що перелік кримінальних правопорушень, до яких можна застосовувати термінове збереження інформації (згідно ст. 176, ч. 3 ст. 190, ст.ст. 200, 231, 300, 301, розділ XVI Особливої частини Кримінального кодексу України), є незаслужено обмеженим. Натомість конвенційну практику рекомендується застосовувати для будь-яких кримінальних правопорушень, незалежно від їхнього ступеня тяжкості чи об'єкта посягання [356, с. 9]. Це можливе не лише через мінімальний вплив на права і свободи людини при його застосуванні, але і справедливе, враховуючи необхідність використання таких цифрових даних не лише під час розслідування зазначених злочинів.

По-друге, вислів «обґрунтовані підстави вважати», оскільки він має оцінний характер, повинен бути пов'язаним з відповідним пунктом мотиваційної частини рішення, який, з невідомих причин, відсутній у статті 1662 (Вимоги до постанови прокурора, слідчого про термінове збереження інформації).

По-третє, не можна проігнорувати термінологічний аспект аналізованого нормативного акта. Наприклад, вираз «власник, володілець або утримувач інформації» з точки зору цивільного права не має сенсу, оскільки право власності, правомірність володіння та обов'язок утримання є майновими поняттями (ч. 1 ст. 316, ч. 1 ст. 317, ч. 1 ст. 322 Цивільного кодексу України), тоді як інформація не є майном (ч. 1 ст. 190 ЦК) і є немайновим благом (ст. 200 ЦК). Крім того, складно уявити, як може існувати таке правовідносини між особою і інформацією. Для виправлення цієї ситуації існують два можливих шляхи: а) змінити об'єкт права і замінити інформацію на матеріальний носій, вказавши володільця або власника пристрою; б) використовувати інший термін для позначення особи, наприклад, «особа, яка обробляє цифрові дані», «особа, яка має доступ до цифрових даних», «особа, яка контролює цифрові дані». Автор віддає перевагу першому підходу, який, крім того, варто застосувати також у статті 1651 і пунктах 2 і 3 статті 1661 КПК в редакції проєкту № 4003.

Також варто відзначити недоліки термінології в переліку цифрових категорій, які наведені в КПК України:

1. електронна інформаційна система або її складова;

2. мобільний термінал засобів зв’язку;

3. інформаційна (автоматизована) система;

4. телекомунікаційна система;

5. інформаційно-телекомунікаційна система.

6. Перші два терміни мають виключно процесуальну спрямованість, оскільки вони не використовуються в інших нормативних документах і залишаються піддаються інтерпретації з боку судової практики через їх недостатнє визначення [232]. Навпаки, останні три терміни не тільки використовуються в інших нормативних актах, але й конкретно визначаються в них (згідно зі ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»). Якщо в чинній редакції процесуального закону різноманітність термінології можна пояснити неузгодженістю змін, то наявність усіх цих варіантів свідчить про наявність принципових відмінностей між першим (електронна інформаційна система або її складова, мобільний термінал засобів зв’язку) і другим (інформаційна (автоматизована) система, телекомунікаційна система, інформаційно-телекомунікаційна система) «поколіннями» категорій. Здається, необхідно остаточно визначитися з термінологією, яка використовується для позначення пристроїв для обробки цифрових даних, стандартизувавши її як на загальній, так і на галузевій основі. Відсутність різниці в процедурі доступу до будь-якого з виділених пристроїв дозволяє використовувати для них єдиний термін, який відображатиме загальну особливість – цифровий характер оброблюваних даних. Можливим варіантом є використання одного з таких термінів: «пристрій для обробки цифрових даних», «сховище цифрових даних», «накопичувач цифрових даних», «носій для збереження цифрових даних», «машинний носій». Ця пропозиція стосується всіх норм, в яких згадуються вказані на початку категорії (у проєкті № 4003 такими є п. 3 ч. 1 ст. 1641, ст. 1661–1664, абз. 2,3 ч. 6 ст. 236).

Є певні застереження стосовно положень, які визначають визначення термінового збереження в процесуальному законодавстві. Зокрема, останній абзац частини 1 статті 1661 КПК у редакції проєкту № 4003 має наступні недоліки:

а) термін «невідкладне збереження інформації» не відповідає назві самого заходу – «термінове збереження інформації».

б) за будь-яких обставин термін термінового збереження не повинен перевищувати строку досудового розслідування.

в) встановлення верхньої межі термінового збереження (дев'яносто днів) може бути занадто тривалим для обґрунтування «часу, необхідного для тимчасового доступу до терміново збереженої інформації» (абзац 1 частини 1 статті 1661), який, в цілому, є оперативним заходом, і в більшості випадків може бути введений за рішенням слідчого чи прокурора (згідно з пунктом 3 статті 159 КПК України у редакції проєкту № 4003).

г) тривалість визначеного слідчим чи прокурором терміну має бути обґрунтована в постанові, так само як і необхідність використання термінового збереження інформації, як було вже вказано раніше. Тому абзац 3 частини 1 статті 1661 КПК у редакції проєкту № 4003 може бути сформульований наступним чином: «Термін дії постанови щодо термінового збереження даних встановлюється в межах строку досудового розслідування і не може перевищувати 60 днів», а частина 1 статті 1662 потребує доповнення сьомим пунктом, який має наступний зміст: «7) строк дії постанови із відповідно обґрунтованою тривалістю» [293].

Те ж саме стосується положень, які регулюють продовження строку термінового збереження інформації (стаття 1663 КПК у редакції проєкту № 4003). Положення щодо продовження потребує вдосконалення наступним чином:

1. Другий абзац частини першої цієї статті, який обмежує загальний строк термінового збереження даних максимальними строками досудового розслідування, втрачає сенс, оскільки застосування такого заходу забезпечення, як до початку, так і після закінчення кримінального провадження, є незаконним (окрім випадків затримання особи без ухвали слідчого судді або суду).

2. Друга частина цієї статті, яка встановлює обов'язок зазначити в постанові обґрунтування необхідності продовження строку термінового збереження, бажано доповнити вимогою пояснити причину неможливості отримати доступ до терміново збережених даних протягом строку дії попередньої постанови.

Положення, яке передбачено у частині 2 статті 1661 КПК у редакції проєкту № 4003, щодо «автоматичного» зобов'язання особи, яка обробляє дані, «не допускати розголошення будь-яким способом факту отримання та виконання... постанови протягом часу її виконання» для забезпечення «гнучкості» норми, бажано замінити дискреційним правилом, яке встановлює можливість накласти таке зобов'язання (право накладання) [134, с. 9]

Зберігання конфіденційності факту використання термінового збереження інформації має велике значення. Тому доцільно доповнити перелік вимог до постанови (частина 1 статті 1662 КПК у редакції проєкту № 4003) вказівкою на такий пункт: «розпорядження не розголошувати інформацію про тимчасове збереження даних». Якщо «автоматичне» зобов'язання стане більш привабливим, перелік вимог до постанови все одно буде потребувати доповнення, включаючи пункт щодо інформування особи про обов'язок не розголошувати інформацію. Це має важливе значення як для ефективності заходу, так і для притягнення до відповідальності за розголошення інформації.

Використання електронної форми постанови про термінове збереження інформації (згідно з абзацом 2 частини 6 статті 110 та частиною 3 статті 1661 КПК у редакції проєкту № 4003) може бути кроком вперед. Проте, варто розглянути можливість зазначення назви основного закону в сфері «електронного документообігу та використання електронних документів» (преамбула Закону України «Про електронні документи та електронний документообіг»). Однак, важливо розглянути питання про механізм електронного надсилання постанови, включаючи визначення адреси електронної пошти та програмних додатків для отримання, підтвердження факту отримання та ознайомлення особи з її змістом.

Для запобігання аналогічним проблемам в сфері цифрових даних потрібно: а) вважати здійснення тимчасового доступу до терміново збереженої інформації підставою для завершення застосування цього заходу забезпечення, оскільки він виконав свою функцію; б) визначити, що підставою для завершення є винесення постанови про закриття кримінального провадження, про що слідчий і прокурор зобов'язані сповістити особу негайно, але не пізніше наступного робочого дня після прийняття цієї постанови, у письмовій або електронній формі. В такому випадку активні дії (повідомлення про рішення), які можуть супроводжувати ризик невиконання, будуть потрібні лише в одному із двох випадків – при закритті кримінального провадження. Також важливо визначити строк для виконання слідчим і прокурором іншого обов'язку – надіслати копію постанови про термінове збереження інформації, постанови про продовження строку або скасування термінового збереження (частина 3 статті 1664 КПК у редакції проєкту № 4003).

Оптимальним строком для цього можна вважати не більше одного робочого дня.

Крім того, Конвенція визначає дані про рух інформації як будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені цією системою та мали відношення до передачі даних, включаючи інформацію про походження, кінцевий пункт, маршрут, час, дату, обсяг та тривалість комунікації, або тип основної послуги (згідно зі статтею 1 Конвенції). Запропонований проєкт № 4003, однак, введе механізм, який лише віддалено нагадує конвенційний. У внутрішньому тлумаченні, часткове розкриття даних було перетворене на тимчасовий доступ до інформації, яка:

а) була об'єктом термінового збереження;

б) не містить персональних даних або не є результатом приватного спілкування (згідно з частиною 3 статті 159 КПК у редакції проєкту № 4003). Однак, в контексті цієї внутрішньої інтерпретації, лише обмежено визначено, які конкретні дані можуть бути тимчасово розкриті, і то в сформульованих досить загальних термінах [131].

Крім того, процедура термінового збереження може стосуватися різних видів інформації, яка не обмежується тільки даними про рух інформації. Це може створити труднощі в досягненні головної мети, яка полягає в оперативному визначенні наступного призначення постанови про термінове збереження під час тимчасового доступу. Перехід до письмової форми постанови також може завадити оперативності, і в цьому випадку немає обов'язкових виключень, які пропонувалися для рішень про термінове збереження (згідно зі статтею 110, частиною 6 КПК в редакції проєкту № 4003). Замість цього, окремі приклади впровадження статті 17 Конвенції свідчать про потребу встановлення уніфікованих правил для термінового збереження і навіть можливості автоматичного та спільного їх застосування (наприклад, в Румунії і Португалії) [356, с. 51].

На національному рівні також можна виявити невідповідності. По-перше, механізм тимчасового доступу до інформації не узгоджується з основною суттю інституту тимчасового доступу до речей і документів та їх носіїв. Зміни, які суперечать основній ідентифікаційній рисі заходу, що повинен мати характер забезпечення [289, с. 72].

Отже, це передбачає доступ не до саміх доказів, а до їхніх процесуальних джерел, і такі зміни не повинні бути обмежені лише конкретними випадками. У випадку визнання необхідності введення цих положень (про що автор має серйозні сумніви), зміни повинні охопити весь механізм тимчасового доступу або нормативне «середовище», в якому цей механізм імплементується, за межами останнього.

По-друге, нова версія пункту 7 частини 1 статті 162 КПК, яка передбачає зміну ознак інформації, що знаходиться у операторів та провайдерів телекомунікаційних послуг, для її віднесення до законної таємниці, дублює низку положень КПК. Це означає, що ті самі обмеження вже закріплені в інших частинах КПК, наприклад, в пункті 7 цієї ж частини статті, які визнають персональні дані особи як частину законної таємниці, а також в частинах 1 та 3 статті 258 КПК, які забороняють доступ до приватного спілкування без розпорядження слідчого судді. Хоча зміни в пункті 7 частини 1 статті 162 КПК є раціональними з точки зору забезпечення оперативності, оскільки вони дозволяють доступ до інформації, яка не є персональними даними або приватним спілкуванням, без розпорядження слідчого судді, визнання їх такими з точки зору прав людини видається складним завданням. Ось через те, що нова версія пункту 7 частини 1 статті 162 КПК дозволяє доступ до приватного спілкування (як частини законної таємниці) під час тимчасового доступу до речей та документів без урахування важкості вчиненого правопорушення – такої важливої гарантії, закріпленої в принципах таємниці спілкування (частина 2 статті 14 КПК). Тому підтримати таку формулювання пункту 7 частини 1 статті 162 КПК не можна. Замість цього в ньому варто найкраще зазначити виключення щодо даних про рух інформації в розумінні, закладеному в статті 1 Конвенції.

По-третє, існують недоліки в нормі, яка регулює виконання постанови про тимчасовий доступ до терміново збереженої інформації (ст. 1651 КПК у редакції проєкту № 4003). Ця норма встановлює, що єдиним способом отримання такого доступу є вилучення копії інформації (частина 1). Але, в той же час, частина 3 цієї ж статті покладає на слідчого чи прокурора обов’язок залишити «опис інформації, яка була вилучена шляхом копіювання». Навіть при тому, що вираз «вилучити шляхом копіювання» досить популярний у судовій практиці [80], таке формулювання складно визнати вдалим

через те, що копіювання і вилучення – це різні способи здійснення тимчасового доступу до речей і документів [183, с. 240].

Вилучення інформації призводить до того, що особа втрачає можливість отримати до неї доступ, що може бути важко пояснити, зокрема через широкий обсяг даних у цифровому середовищі. Тому більш прийнятним здається таке формульовання: «...опис інформації, яка була скопійована відповідно до постанови».

Обшук. Причина, що стоїть за цією пропозицією, полягає в бажанні розширити можливості проведення цифрового обшуку, відповідно до положень пунктів 2 та 4 статті 19 Конвенції [230]. Водночас національна інтерпретація конвенційного заходу породжує низку питань і зауважень як у міжнародному, так і національному контекстах. По-перше, не визначено територіальні обмеження для доступу до іншої інформаційної системи, незважаючи на важливість принципу знаходження цієї системи на території нашої держави [370]. У разі транскордонного характеру цифрового доступу, Конвенція, у зусиллях збереження суверенітету інших держав та прав і свобод осіб, які перебувають на їхній території, вказує на необхідність використання міжнародних механізмів співробітництва (згідно зі статтями 31 та 32 Конвенції). По-друге, абзац 2 частини 6 статті 236 проєкту № 4003 передбачає розширення меж обшуку, проте ця ідея може бути викликана певною складністю та навіть суперечливістю. Наприклад, виникає питання про легальність доступу до віддаленого цифрового пристрою. По-третє, ця норма має потенційні ризики для прав і свобод осіб. Вона дозволяє обійти системи логічного захисту незалежно від мети обшуку та об’єкта пошуку. До того ж, підставою для доступу до віддаленої інформаційної системи визнається сформульовання, яке надає широкий діапазон повноважень виконавцям обшуку, основою якого є відповідність інформації «встановленню обставин кримінального провадження» (абзац 2). Такий підхід може призвести до ситуації, де слідчий або прокурор, отримавши дозвіл на обшук житла або іншого володіння особи, матиме можливість досліджувати зміст всіх цифрових пристроїв, включаючи логічні системи захисту та акаунти в соціальних мережах, просто тому, що доступ до них фізично здійснюється на місці обшуку. У цьому контексті може бути недостатнім судовий контроль, який не здійснюватиметься належним чином з погляду оцінки правомірності втручання в інші, крім права на недоторканість житла, права (наприклад, права на таємницю спілкування). Також, надання особі,

права і свободи якої були обмежені, можливості оскаржити такі дії, не передбачається компенсаційним механізмом. Важливо зауважити, що такий рівень втручання в права та свободи людини не повинен відбуватися без судового контролю, як попереднього (надання прямого дозволу на пошук конкретної інформації чи пристрою) або подальшого (для оцінки правомірності доступу до інформації чи пристрою, які не були вказані в судовому дозволі, після втручання). Варто зазначити, що ефективні механізми контролю цифрового втручання можна знайти в судовій системі Сполучених Штатів Америки, включаючи концепцію розумного очікування щодо приватності та принцип «закритого контейнера» [383].

Наявність детальних норм для регулювання цифрових дій обвинувачення, зокрема впровадження нового слідчого заходу – цифрового обшуку, є важливою для вирішення проблем, що виникають. Це дозволить досягти якісного вирішення порушених питань. По-четверте, у запропонованому формулюванні абзацу 3 частини 6 статті 236 КПК у редакції проєкту № 4003 відсутній зміст: він надає право, а не обов'язок осіб повідомляти інформацію щодо особливостей роботи та захисту цифрових пристроїв, на відміну від конвенційного правила, яке вимагає надання такої інформації (згідно з пунктом 4 статті 19 Конвенції).

З вищенаведеного можна зробити висновок, що імплементація положень Конвенції є необхідною і очевидною. Однак запропоновані проєктом № 4003 механізми потребують суттєвої переробки. Поміж зазначеними вище зауваженнями та пропозиціями також слід розглянути додаткові шляхи поліпшення процесуальних механізмів, такі як:

1. впровадження часткового розкриття даних про рух інформації як складової частини термінового збереження даних;
2. об'єднання у одному заході забезпечення – збереження цифрових даних, як термінове збереження та часткове розкриття даних (статті 16, 17 Конвенції), так і арешту цифрових даних після отримання до них доступу (пункт 3 статті 19 Конвенції) – для збереження цифрового оригіналу;
3. надання права застосовувати захід забезпечення не лише слідчим, прокурорам під час досудового розслідування, але і суду під час судового провадження (на прикладі практики Угорщини, Португалії, Румунії, Словаччини та інших держав) [356];

4. Встановлення кримінальної відповідальності за порушення збереження чи розкриття даних: а) Передбачення кримінальної, а не адміністративної відповідальності; б) Розширення відповідальності не тільки на фізичних осіб, але й на юридичних осіб;

Для досягнення мети термінового збереження в разі загрози активному опору володільця цифрового пристрою внесення можливості негайного проведення цифрового обшуку [370] із подальшим судовим контролем за його правомірністю.

Однак, вищенаведені спостереження та пропозиції можуть бути розглянуті як спроба спонукання до наукового обговорення та розробки способів реалізації інших положень Конвенції. Це може призвести до плідної взаємодії між вченими, практиками та законодавцями [293].

4.3. Формування моделі забезпечення інформаційної безпеки в мережі internet на основі позитивного досвіду зарубіжних країн

У сучасний час Україні особливо важливо забезпечити інформаційну безпеку, що стосується як численних атак на національний інформаційний простір з боку інших країн і їх контрольованих суб'єктів, так і активізації процесів євроінтеграції України та участі держави в міжнародних безпекових заходах та програмах, які підтримуються Сполученими Штатами Америки та іншими країнами.

Для України перехід до нового етапу суспільного розвитку означає невід'ємну ситуацію, в якій поліпшення організації використання інформаційної основи для розвитку української нації і держави – це об'єднана система вітчизняних інформаційних баз, а також розвиток інформаційного виробництва та систем соціальних інформаційних комунікацій, що у сукупності утворюють ресурсну базу вітчизняного інформаційного простору, – може гарантувати належні позиції в міжнародному співробітництві.

Ключовим аспектом цього розвитку є організація безпеки національного інформаційного суверенітету для України як об'єкта глобальних інформаційних впливів, а також як повноправного суб'єкта міжнародної діяльності, міжнародних обмінів інформацією. Це має надзвичайно важливе значення для існування та розвитку національних інформаційних ресурсів в умовах глобальних впливів.

Ефективна інформаційна безпека нашого суспільства є гарантом цього процесу [187, с. 112].

У цьому випадку об'єктом інформаційного суверенітету є суверенні інформаційні ресурси, що представляють собою обсяги інформації, необхідні для існування та розвитку нації або держави. Суверенні інформаційні ресурси є результатом накопичення досвіду і знань українського народу у поточному і попередніх поколіннях, що є основою для його існування і розвитку. Вони забезпечують збереження національно-культурної самобутності в умовах глобалізації і визначають рушійні сили сучасного національного інфопростору.

Безпека національних інформаційних ресурсів та технологій є одними з найважливіших чинників забезпечення національних інтересів країни. Впровадження інновацій, заснованих на наукових і технологічних досягненнях, є основою підвищення національного добробуту. Реалізація успішної інформаційної політики може суттєво вплинути на зниження напруженості в економічній та соціальній ситуації в країні та сприяти вирішенню зовнішньополітичних конфліктів.

Паралельно з цим виявляється, що поняття «інформаційні ресурси» потребує належного теоретичного й правового обґрунтування. Національні інформаційні ресурси становлять основу інформаційного суверенітету, через них держава контролює й регулює інформаційні потоки. Це ключовий елемент людської діяльності. У сучасних наукових дослідженнях цей ресурс розглядається в двох аспектах. Загальномашиною інформаційний ресурс є важливим засобом, джерелом соціальних змін. У конкретному значенні це є продуктом виробництва та обміну, об'єктом конкуренції і суперництва, сировиною для цілеспрямованої (раціональної) соціально-економічної діяльності людини, під час якої формується інформаційний (інтелектуальний) продукт та задовольняються потреби та інтереси людини.

Отже, суть інформаційного ресурсу полягає в системі або сукупності засобів задоволення інформаційних потреб людини. Як будь-яка система, інформаційні ресурси та інформаційна інфраструктура постійно змінюються, а разом з цим змінюється й їхній зміст.

Процеси глобалізації, спровоковані, зокрема, інформатизацією на основі електронних технологій, крім свого позитивного впливу на

прогрес, породжують нові виклики і загрози для інформаційної інфраструктури, національного інформаційного суверенітету, культурної ідентичності, самосвідомості. Ці виклики відзначаються множинними можливостями для подальшого розвитку цивілізації. Тому робота з нейтралізації кіберзагроз, як важливої складової забезпечення інформаційної безпеки, є запорукою ефективного використання та перспективного розвитку національних масивів інформації для кожної держави та нації.

Питання забезпечення інформаційної безпеки мають надзвичайну важливість для сучасної української держави. Це особливо актуально через необхідність протистояти незаконним атакам на інформаційний простір України, збереження інформаційних ресурсів та захисту населення від негативного впливу інформації. Крім того, ключовим пріоритетом зовнішньої політики України є європейська інтеграція. Це передбачає потребу в удосконаленні нормативно-правової бази забезпечення інформаційної безпеки України, яка відповідає не лише міжнародним стандартам, але й основним українським національним інтересам в інформаційній сфері. Ці аспекти відображені у Стратегії Національної безпеки України [303].

У своїх засадах Стратегія визначила основні напрямки державної політики національної безпеки, наголошуючи на важливих цілях, зокрема: зменшенні загроз державному суверенітету, створенні умов для відновлення територіальної цілісності України у межах визнаних міжнародних кордонів, гарантуванні мирного майбутнього як суверенної і незалежної, демократичної, соціальної та правової держави; утвердженні прав та свобод людини і громадянина, забезпеченні нового рівня економічного, соціального та гуманітарного розвитку, інтеграції України до Європейського Союзу та утворенні умов для приєднання до НАТО. Більш того, Стратегія вказала на ключові загрози інформаційній безпеці, такі як проведення інформаційної війни проти України, відсутність єдиної комунікативної політики держави та низький рівень медіакультури суспільства. Це підкреслює актуальність даної теми для подальших досліджень [297].

Так, оскільки потрібно удосконалити нормативно-правове забезпечення та запобігти та нейтралізувати потенційні й реальні загрози національній безпеці в інформаційній сфері, у зв’язку з розпочаттям гібридної війни проти України, була виявлена

необхідність кардинальних змін у системі забезпечення інформаційної безпеки нашої держави. Основні заходи були запроваджені згідно з рішенням Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо удосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», яке було затверджено Указом Президента України від 1 травня 2014 року № 449/2014 [257].

Відповідно до вказівок у цьому рішенні, Кабінет Міністрів України отримав завдання розробити та внести до розгляду парламенту законопроекти щодо внесення змін до законів України з метою протидії інформаційній агресії іноземних держав. Ці зміни передбачали, зокрема, визначення механізмів протидії негативному інформаційно-психологічному впливу, включаючи заборону ретрансляції телевізійних каналів, та впровадження системи інформування та захисту журналістів іноземних ЗМІ, які працюють у зоні збройних конфліктів та терористичних актів. Крім того, наказувалося розробити стратегію розвитку інформаційного простору України, впровадити організаційні, інформаційні та роз'яснювальні заходи для всебічного освітлення реалізації державної політики у сфері забезпечення інформаційної безпеки та зміцнення контролю над дотриманням законодавства у сфері інформаційно-психологічної та кібернетичної безпеки. Згідно з цим планом заходів була розроблена Доктрина інформаційної безпеки України [258].

Розробка ефективних засобів гарантування національної інформаційної незалежності є ключовою для прогресу суспільства та актуальним завданням нашого часу. Забезпечення кібернетичної безпеки є критично важливим для України на сучасному етапі розвитку. Це особливо актуально через необхідність протистояти незаконним втручанням у інформаційний простір України, збереження цінних інформаційних ресурсів та захисту населення від шкідливого впливу інформації та інших негативних аспектів. Крім того, стратегічний пріоритет зовнішньої політики України – це інтеграція в Європейський союз. Це вимагає вдосконалення нормативно-правової бази забезпечення кібернетичної безпеки України, яка відповідає не лише міжнародним стандартам, але й українським національним інтересам в галузі інформаційної сфери [208].

Поразка в інформаційній, включаючи кібернетичну, війні, може неодмінно призвести до розпаду будь-якої країни. У сучасних

умовах багато важливих систем промислового і оборонного секторів економіки, наприклад системи управління повітряним сполученням, підприємства енергетичної та атомної галузей та електромережі, які працюють на основі інформаційно-комунікаційних технологій, є потенційними об'єктами ризику через їхню уразливість для зовнішніх вторгнень.

Отже, до зовнішніх загроз у кібернетичному просторі відносяться, зокрема, хакерські атаки, які здійснюються з територій інших держав і спрямовані на порушення роботи комп'ютерних систем, крадіжку конфіденційної інформації тощо [101, с.12].

Фактором, який призводить до ослаблення можливостей держави нейтралізувати загрози, є зростання взаємозалежності між країнами та їх вразливість перед зовнішніми впливами. У більшості випадків держава втрачає свій монопольний характер на власній території, її інформаційна політика все більше обмежується, піддається корекції та упливу з боку інших країн, міжнародних та недержавних організацій, неформальних асоціацій з негативним спрямуванням, злочинних угруповань тощо. У випадку слабкої ідеологічної, інституційної та економічної бази держава не має можливості використовувати технологічні, економічні та соціокультурні переваги глобалізації, проте вона активно усмоктує її негативні аспекти [213].

Розвиток глобальних процесів, заснованих на широкому впровадженні інформаційних технологій, призводить до збільшення різноманітності загроз у сфері інформаційної безпеки. Це може охоплювати конкуренцію на внутрішньому інформаційному ринку між вітчизняними продуктами та більш конкурентоспроможними, аж до проведення цілеспрямованих інформаційних війн. За доповіддю Національної ради з розвідки США, інформаційні війни стануть домінуючим фактором у поточному столітті, охоплюючи всі рівні соціальної структури, включаючи міждержавні конфлікти. У сучасних умовах інформаційна революція спостерігається на тлі інформаційних війн, спрямованих на підрив національної безпеки держав. З цими уявленнями безпекова роль держави в глобальних регіонах світу набуває надзвичайної важливості [215].

Поточна ситуація в світовому інформаційному просторі може бути описана таким чином:

– Більшість країн світу стикаються з проблемами кібертероризму, кіберзлочинності та інших аспектів інформаційної безпеки.

– Протягом останніх десятиліть спостерігається поширення інформаційної агресії та насилля.

– Зростає поширення агресивної реклами, спроб маніпуляції свідомістю людини та проведення інформаційно-психологічних операцій.

– Приблизно в 120 країнах світу (за оцінками американських експертів) ведуться розробки інформаційної зброї або її компонентів (у порівнянні – розробки зброї масового знищення здійснюються у близько 20 країнах).

– Наслідки використання сучасної інформаційної зброї (згідно з висновками вчених та експертів європейських країн, України і США) можна порівняти з використанням зброї масового ураження.

– Сучасні виклики та загрози в інформаційній сфері представляють реальну загрозу для безпеки людства та міжнародного право-порядку [223, с. 3].

Можна говорити про важливість та актуальність посилення регулювання на національному та міжнародному рівнях у кіберпросторі, а також про зростання ролі приватного сектора. Необхідно встановити контроль над кіберзброєю та посилити охорону критичної інфраструктури України. Інновації в галузі кібербезпеки та вдосконалення освітніх програм для підготовки фахівців у цій сфері також важливі.

Проте без системного та комплексного підходу всі згадані заходи не забезпечать необхідного рівня кібербезпеки, а отже, національної безпеки України в цілому, на новому якісному рівні.

Запобігання злочинності у сфері інформаційних технологій повинно бути системним, враховуючи сучасні ризики та виклики у кіберпросторі. Інституційне середовище, яке забезпечує кібер-безпеку, повинно постійно удосконалюватися. Ефективність заходів у цій сфері слід досягати шляхом оцінки загроз організованій кіберзлочинності для ідентифікації сучасних загроз та ризиків у кіберпросторі.

У сучасному глобалізованому світі Україні потрібна адекватна система кібернетичної безпеки.

Активність провідних держав у кіберпросторі, глибинні зміни у внутрішній інформаційній політиці та формування потужних транснаціональних злочинних груп, що спеціалізуються на кіберзлочинах, вимагають перегляду пріоритетів у вітчизняному секторі кібербезпеки з урахуванням вищезазначених тенденцій.

Важливо зауважити, що в умовах швидкоплинних змін у суспільному житті та революційного розвитку інформаційних технологій значна частина чинних нормативних актів, як на внутрішньодержавному, так і на міжнародному рівні, втрачає актуальність та відповідність процесам, які вони регулюють, і потребує уточнень або перегляду. Розвиток інформаційної діяльності вимагає правового урегулювання нових аспектів цієї діяльності.

Необхідно мають бути чітко визначені правові основи для оптимізації боротьби з кібертероризмом в умовах активізації глобальних впливів та розширення нових інформаційних технологій. Комплекс відповідних правових актів повинен постійно удосконалюватися, враховуючи міжнародне законодавство та еволюцію вітчизняної законотворчої практики. Це має бути відповідальною місією на збереження національних інтересів в галузі інформаційної діяльності.

У контексті правового регулювання, спрямованого на реалізацію функцій держави, зокрема у забезпеченні кібербезпеки та протидії кіберзагрозам, важливо надати пріоритет загальній безпеці суспільства. Особливу увагу слід приділяти правовим нормам, що забороняють певні дії, особливо відносно передвстановлених деструктивних технологій. Однак основна проблема полягає у складності оцінки потенційно деструктивного впливу технологій та можливих помилок у їхній оцінці. Тому важливо продовжувати дослідження у галузі правової науки для знаходження шляхів вирішення цих проблем [336, с. 312].

Крім того, регулювання використання емерджентних технологій повинно обмежуватися реалізацією економічних функцій держави, спрямованих на забезпечення економічної різноманітності, як це передбачено в статті 15 Конституції України. Необхідно сприяти вільному ринковому господарству та забезпечувати державний вплив для запобігання зловживання монопольним положенням та обмеження економічної конкуренції. Пріоритети та переваги мають бути обґрунтованими і випливати із реальних потреб.

Оскільки існуючі наразі інформаційні технології дозволяють як приховувати розташування, так і використовувати дані інших осіб, слід розглянути такі кроки:

На національному рівні:

1. Виступати та брати участь у розробці міжнародної стратегії щодо протидії кіберзагрозам і створення єдиних міжнародно-правових механізмів для регулювання віртуального простору.

а) Спільною метою та напрямком Стратегії кібербезпеки є забезпечення віртуальної безпеки особистості, організацій та держави шляхом визначення системи пріоритетів, принципів та заходів у сфері внутрішньої та зовнішньої політики. В цій стратегії повинні бути відображені всі аспекти кіберпростору, які забезпечують захист від максимально можливої кількості загроз та негативних впливів.

б) Для конкретизації приватних напрямків Стратегії кібербезпеки необхідно визначити стандарти співпраці суб'єктів інформаційного суспільства – особистості, організацій та держави – у сфері забезпечення кібербезпеки. Це повинно включати норми встановлення відповідальності за недотримання вимог кібербезпеки, уникання надмірних обмежень, а також надання пріоритету ризикам кібербезпеки відповідно до можливостей реалізації кіберзагроз та масштабів негативних наслідків від інцидентів кібербезпеки. Також потрібно актуалізувати засоби та методи забезпечення кібербезпеки для протистояння постійно змінюваним кіберзагрозам [346, с. 244].

– створити та впровадити інституційну систему кібербезпеки з різними рівнями, що включають:

1. Рівень наукового аналізу, який досліджуватиме ризики кібербезпеки відповідно до можливих кіберзагроз та наслідків, актуалізуватиме засоби та методи забезпечення кібербезпеки. Це є одним із найважливіших завдань. Оскільки проблема полягає в складності класифікації загроз, що виходять як з території держави, так і виникають безпосередньо в межах держави, важливо наголосити на необхідності для будь-якої держави розробити стратегію ідентифікації кіберзагроз, а також їх вчасного виявлення, запобігання, захисту та мінімізації наслідків.

2. Виконавчий рівень, що координуватиме дії в двох напрямках: внутрішньому (між національними структурами, відповідальними за виявлення та протидію кіберзагрозам) та зовнішньому, коли координація здійснюється між національними структурами та аналогічними міжнародними організаціями.

– посилення потужностей у сфері інформаційної безпеки для протидії електронним атакам.

Необхідно посилити внутрішньополітичні заходи для сприяння розвитку технологічного аспекту кібербезпеки з метою збереження рівноваги та створення противаги потенційним «супротивникам» у сфері кібербезпеки.

На рівні міжнародного співробітництва:

– виступати за впровадження та реалізацію міжнародного співробітництва в галузі кібербезпеки, відстеження діяльності злочинних, терористичних груп та окремих хакерів, які активно діють у кіберпросторі;

– активно брати участь у формуванні та розвитку міжнародних структур, спрямованих на виявлення кіберзагроз, своєчасне їх виявлення, запобігання та захист, а також мінімізацію наслідків.

На міжнародному рівні:

– сприяти створенню та впровадженню міжнародних угод у сфері запобігання та розслідування кіберагресії, а також оновлювати наявні нормативно-правові акти.

– започаткувати утворення міжнародного органу з регіональними представництвами, який є аналогом ООН у кіберпросторі, отримавши назву «КіберООН» (далі – КООН). В цьому органі мають існувати різні підрозділи, такі як науково-аналітичний рівень, який здійснюватиме аналогічні функції національного рівня, і виконавчий рівень, який може функціонувати на міжнародному, регіональному та національному рівні. Регіональний рівень дозволить швидко залучати ресурси для протистояння кіберагресіям. Національний рівень дозволить представникам КООН спільно з місцевими національними представниками здійснювати розслідування подій на регіональному та міжнародному рівнях. Додатково, важливо, щоб керівництво КООН складалося з 12 адміністраторів, які щорічно обираються з членів органу. На відміну від ООН, в КООН не передбачено осіб з правом вето або постійних членів. У випадку кіберагресії КООН сформує комісію для розслідування, включаючи міжнародних, регіональних та національних представників. Висновки комісії разом із відповідними доказами будуть передані до міжнародного суду.

На нашу думку, створення такого органу як КООН дозволило б сформувати систему міжнародних стандартів в сфері боротьби і запобігання кіберзлочинам, а також гарантувати безпеку у кіберпросторі у всьому світі.

Аналіз розвитку інформаційного суспільства, інформаційної глобалізації та протистояння в інформаційній сфері сучасних умов

виявив ряд проблем організаційно-правового характеру у сфері інформаційної безпеки України, зокрема:

– Недостатній розвинутість стратегічного рівня забезпечення інформаційної безпеки.

– Низький рівень інформаційного супроводження зовнішньої та внутрішньої політики України.

– Фрагментарність та недостатня координація діяльності державних органів та установ, які відповідають за забезпечення інформаційної безпеки.

– Неіснуючість ефективних механізмів експертної оцінки інформаційної продукції, яка може загрожувати правам людини, інтересам суспільства та держави.

– Недостатня активна участь громадськості та приватного сектору України у протидії негативним інформаційним впливам та міжнародній співпраці у цьому напрямку.

– Прогалини в законодавстві та організаційні проблеми у сфері обігу інформації з обмеженим доступом.

У сучасний період виклики, що виникають у сфері інформаційної безпеки України, обумовлені внутрішніми та зовнішніми чинниками. Внутрішні фактори включають передусім відсталість у сфері інформаційних технологій в Україні порівняно з провідними країнами світу, низький рівень інформатизації, розпорошеність повноважень державних органів та недоліки у законодавстві щодо інформаційної сфери. Зовнішні виклики пов’язані з глобальними тенденціями у створенні та використанні інформаційних технологій, а також спробами зовнішніх суб’єктів впливати на світовий та вітчизняний інформаційний простір для захисту своїх інтересів, а також залежність від іноземного програмного забезпечення [297].

Однією з основних тенденцій сучасного суспільства є загальна інформатизація, яка охоплює майже всі сфери людської діяльності, включаючи економіку, державне управління, науку та мистецтво. Цей процес відображає перехід цивілізованого світу до нового технологічного етапу, який характеризується як інформаційне суспільство. Додатково, важливо відзначити постійне зростання темпів розвитку цифрової економіки, які в декілька разів перевищують показники всіх інших галузей виробництва [67, с. 167].

У контексті глобальної інформатизації відбуваються зміни у способі формування сучасних правовідносин у сфері поширення інформації. Це включає переосмислення суті, змісту, ролі та місця

організаційно-правових засад захисту інформації, зокрема тієї, яка є обмежено доступною, такої як інформація, пов'язана з правоохоронною діяльністю та забезпеченням громадського порядку [292, с. 5–6]. Однак становлення інформаційного суспільства в Україні стримується низкою проблем нормативно-правового та організаційного векторів [67, с. 39].

У контексті глобалізації стрімкий прогрес інформаційних технологій, нових систем комунікацій та комп'ютерних мереж викликає недобросовісне використання цих засобів кримінально протиправним чином. Тому важливим є вивчення та адаптація міжнародного досвіду передових країн у галузі державної діяльності, спрямованої на правове регулювання захисту інформації у сучасних умовах та запобігання злочинності у сфері інформаційних технологій. Це має важливе значення для досягнення стратегічних цілей України у контексті європейської та євроатлантичної інтеграції [292, с. 5–6].

Так, Ю. Є. Максименко зауважує, що перехід до інформаційного суспільства призводить до різних наслідків, які мають як позитивний, так і негативний характер. З одного боку, спостерігається швидка передача та обробка значної кількості інформації. З іншого боку, серйозне хвилювання викликає розповсюдження незаконного збору та використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації у електронних системах, викрадення даних з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах, маніпулювання суспільною та індивідуальною свідомістю тощо. Суспільство, що переходить до інформаційного, перетворює статус інформації, яка сьогодні може бути як засобом забезпечення безпеки, так і загрозою та небезпекою [195, с. 1].

Безсумнівно, у сучасній епосі розвитку людського суспільства великою стратегічною цінністю, яка вимагає захисту, є інформація. Вона охоплює широкий спектр від простих даних про громадян країни до стратегічних державних програм. Однак ці дані все частіше стають об'єктом зловживань та злочинних втручань. Використання інформаційних технологій на основі особистих комп'ютерів, мереж та комп'ютеризованих комунікаційних систем в широкому масштабі відкрило перед людством новий етап розвитку

– інформаційне суспільство. Це призвело до появи нового виду проблеми – комп'ютерної або кіберзлочинності.

Один з потенційних підходів до протистояння кіберзлочинності на міжнародному рівні та розвитку міжнародного співробітництва полягає в створенні та стандартизації відповідної нормативно-правової основи. Першими документами у цьому контексті стали Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 року [166], та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р. [119]. Прийняття цих актів ознаменувало закладення правового фундаменту у сферу захисту свободи, безпеки і прав людини в мережі Інтернет не тільки на регіональному рівні, оскільки Конвенція відкрита для підписання державами, які не є членами Ради Європи [291]. Для багатьох країн, включаючи Україну, кіберзлочинність є актуальним явищем, яке постає внаслідок широкого впровадження сучасних інформаційних та телекомунікаційних технологій в економічні процеси.

Виявлення, розкриття та розслідування «транскордонних» кримінальних правопорушень через глобальну мережу Інтернет стикаються з основними викликами, включаючи розподіленість слідів у різних територіях та їх тимчасове зберігання. Анонімність учасників Інтернету та тимчасовий характер інформації роблять складним встановлення місця вчинення нових кримінальних правопорушень Співпраця між оперативними підрозділами на різних рівнях, включаючи взаємодію з представниками правоохоронних органів інших країн, відіграє важливу роль у підвищенні ефективності оперативного документування кримінальних правопорушень у сфері інформаційних технологій [171, с. 518–519]. Для покращення співпраці передбачено утворення органу на національному рівні згідно з Конвенцією, який буде обслуговувати контакти цілодобово для надання негайної допомоги у розслідуванні або переслідуванні кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або для збирання електронних доказів. Ця допомога може включати сприяння або, за умови дозволу внутрішньодержавного законодавства і практики, пряме здійснення таких заходів:

а) надання технічних консультацій;

б) збереження даних згідно зі статтями 29 («Термінове збереження зберіганих комп'ютерних даних») та 30 («Термінове розкриття збережених даних про рух інформації»);

в) збирання доказів, надання юридичної інформації та встановлення місцезнаходження підозрюваних відповідно до статті 35 [166].

– Конвенцією встановлені обов'язкові вимоги для впровадження в законодавство країн, що приєдналися:

– надання правоохоронним органам повноважень щодо видачі обов'язкових для виконання ухвал про термінову реєстрацію та подальше зберігання комп'ютерних даних, необхідних для розкриття криміналного правопорушення (ч.1 ст.16, ст.17);

– збереження провайдерськими установами даних про трафік інформації на термін до 90 днів з можливістю подальшого продовження цього строку (ч.2 ст.16);

– накладення на суб'єктів, які зберігають комп'ютерні дані, обов'язку не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом періоду, що визначається законодавством країни (ч.3 ст.16, ч.3 ст.20, ч.3 ст.21) [166].

Питання запобігання злочинності у сфері інформаційних технологій є ключовим для органів та інституцій Організації Об'єднаних Націй. Ця проблема активно обговорюється в рамках Генеральної Асамблеї (A/RES 63/195), Економічної і Соціальної Ради (рез. 2009/22), Комісії з попередження злочинності і кримінального правосуддя (док. E/CN.15/2009/15) та конгресів ООН з попередження злочинності і кримінального правосуддя. Ці органи виносять рішення, спрямовані на розробку шляхів та засобів вирішення цієї проблеми. У низці міждержавних нормативно-правових актів також порушуються ці питання [119].

Визнано, що на сьогодні кіберзлочинність становить загрозу не лише національній безпеці окремої країни, але й загрожує всьому людству. Саме тому цей аспект привертає велику увагу в багатьох країнах. Після аналізу досвіду поліції кількох країн у боротьбі з кіберзлочинністю можна відзначити, що це досягається за допомогою додаткового надання функцій існуючим підрозділам поліції або створення спеціальних підрозділів. У багатьох країнах світу, таких як Австралія, Бельгія, Велика Британія, Данія, Естонія, Індія, Канада, Малайзія, Нідерланди, Німеччина, Норвегія, Польща, США, Швейцарія, Швеція та інші, практикується створення

спеціальних підрозділів поліції для боротьби з кіберзлочинністю. Основні функції цих підрозділів включають:

– Моніторинг кіберпростору для виявлення кіберзлочинів, вірусів та шкідливого програмного забезпечення.

– Оперативно-розшукові та розвідувальні заходи для фіксації протиправної діяльності кіберзлочинців.

– Розслідування кіберзлочинів та надання підтримки іншим галузевим службам та правоохоронним органам у межах своєї компетенції.

– Накопичення, узагальнення та аналіз інформації про кіберзлочинність.

– Профілактика кіберзлочинів через співпрацю з громадськістю та засобами масової інформації.

– Навчання працівників поліції.

– Деякі спеціальні підрозділи поліції, що займаються протидією кіберзлочинності (їх також називають спеціальними підрозділами для боротьби з кримінальними правопорушеннями, пов'язаними з використанням інформаційних технологій), виконують додаткові завдання, включаючи:

– Розслідування кіберзлочинів.

– Профілактику та контроль над телекомунікаційними послугами.

– Експертний аналіз доказів, зібраних на електронних носіях.

– Створення та поновлення відповідної бази даних щодо кіберзлочинів.

– Надання банкам послуг забезпечення захисту персональної інформації клієнтів та інше.

Наприклад, в Індії підрозділи, які займаються запобіганням кіберзлочинів, можуть залучати професійних хакерів для їх розкриття. Важливо відзначити, що під час розслідування кіберзлочинів велику увагу приділяють наданню допомоги потерпілому відновленню пошкодженої або втраченої інформації та приймають всі необхідні заходи для збереження доказів у справі [288, с. 193]. Більш того, в останні роки у різних частинах світу було запроваджено кілька власних стратегій для запобігання злочинності у сфері інформаційних технологій.

Європейський Союз виконує координаційну роботу з узгодження законодавства щодо кіберзлочинності, яке діє на території країн-членів цієї організації. Ця робота включає прийняття ряду доку-

ментів, зокрема: Директива No2000/31/ЄС Європейського парламенту та Ради про деякі правові аспекти послуг інформаційного суспільства, включаючи електронну торгівлю на внутрішньому ринку; рамкове рішення Ради Європейського Союзу 2000/41/ЈНА з боротьби з шахрайством та фальсифікацією безготівкових платіжних засобів; рамкове рішення Ради Європейського Союзу 204/68/ЈНА з боротьби з сексуальною експлуатацією тощо (п. 20–21).

Важливо вказати, що для поліпшення правового забезпечення боротьби зі злочинністю у сфері інформаційних технологій в Україні необхідно вивчати позитивний досвід правоохоронних органів інших країн у цьому напрямі. Зокрема, поліція Канади активно бореться з комп'ютерними та телекомунікаційними кримінальними правопорушеннями. Королівська канадська кінна поліція (федеральна поліція, КККП) відповідає за розслідування комп'ютерних кримінальних правопорушень та співпрацює з іншими країнами, користуючись даними канадського поліцейського інформаційного центру. Діяльність цього підрозділу спрямована на розслідування та виявлення протирпавних діянь, пов'язаних з комп'ютерами та телекомунікаціями. Секція захисту інформаційних технологій забезпечує безпеку федеральних державних комп'ютерних центрів та приватного сектору, надає консультації та підготовку персоналу з комп'ютерного захисту. Працівники цього підрозділу надають допомогу поліцейським у розслідуванні кримінальних правопорушень, пов'язаних з комп'ютерними системами. З огляду на швидкість передачі інформації між терміналами, у Канаді працює близько 2500 точок доступу, включаючи 1285 федеральних і провінційних поліцейських відділень. До мережі підключено 1180 спеціалізованих підрозділів КККП для ефективного використання системи [79].

Безсумнівно, ця сфера діяльності поліції є надзвичайно важливою, оскільки збитки в економіці вже досягли значних розмірів, а деякі злочинці ведуть організовану діяльність на міжнародному рівні. У той же час необхідно визнати, що законодавство Канади щодо комп'ютерної злочинності потребує удосконалення. Оскільки завдання, які стоять перед поліційськими у боротьбі з комп'ютерною злочинністю, є міжнародного характеру та не є винятковими для Канади, вони активно співпрацюють з іншими країнами та Інтерполом з метою удосконалення законодавства у цьому напрямку. Розслідування комп'ютерних злочинів є складним

завданням, особливо через фактор часу, оскільки передача даних може відбуватися майже миттєво, і часто важко знайти докази порушення міжнародного законодавства. За інформацією КККП, на сьогодні велика кількість комп'ютерних злочинів вчиняється неповнолітніми до дванадцятирічного віку. Згідно з кримінальним кодексом Канади, для встановлення кримінальної відповідальності необхідно довести несанкціоноване використання комп'ютерної системи та намір особи заподіяти шкоду. Такий підхід вимагає чіткого визначення параметрів доступу до комп'ютерної техніки для запобігання порушень. Необхідно враховувати дані про особи та параметри доступу з обмеженнями, а також можливість службовців «експериментувати» з програмами. Міністерство юстиції чи відповідний підрозділ КККП можуть надати кваліфіковану консультацію щодо можливої неправомірної поведінки у цьому напрямку. Необхідно вказати, що методика розслідування несанкціонованого дистанційного доступу до комп'ютерних мереж технічно складна, і це завдання виконують спеціалізовані поліцейські підрозділи. У зв'язку з загрозою комп'ютерної злочинності, її тенденціями та впливом на світове співтовариство в межах ООН регулярно проводяться симпозіуми з профілактики та припинення комп'ютерної злочинності. Фахівці відзначають програмні методи захисту інформації в комп'ютерних системах колективного користування шляхом вдосконалення системи автоматичного контролю як один із способів. На зменшення злочинів, пов'язаних з незаконним використанням телекомунікаційних систем на міжпровінційному, державному та міжнародному рівнях спрямовані дії та управління з боротьби з економічними злочинами. Інформаційний центр надає допомогу поліцейським підрозділам. Поліцейська діяльність з попередження та розкриття діянь, пов'язаних з кіберзлочинністю, також спрямована на розвиток відносин з різними групами суспільства через засоби масової інформації, консультативні зустрічі з представниками громадськості, співробітництво з органами влади та управління, громадськими організаціями та окремими громадянами. Таким чином, поліція є важливим партнером у співтоваристві відомств, які борються зі злочинністю, зокрема кіберзлочинністю, і забезпечують дотримання прав людини та захист федеральних державних комп'ютерних центрів і приватного сектора [79].

Необхідно підкреслити, що успішне запобігання злочинності у сфері інформаційних технологій вимагає ефективного та добре організованого співробітництва між правоохоронними органами різних країн, включаючи співпрацю в межах Інтерполу. Погоджуємося з точкою зору вчених, таких як В. В. Коряк та В. Р. Сливенко щодо визначення взаємодії в правоохоронних органах як узгодженої в часі, методах і засобах діяльності підрозділів (або працівників), які не підпорядковані один одному напряму, з метою досягнення загальних цілей та вирішення поставлених завдань.

Зважаючи на специфіку кримінальних правопорушень у галузі інформаційно-комунікаційних технологій, ефективність оперативного документування цих протиправних діянь значно залежить від співробітництва правоохоронних органів на всіх рівнях:

1. у внутрішньовідомчому плані – з іншими оперативними підрозділами кіберполіції, науково-дослідними експертно-криміналістичними центрами та слідчими підрозділами;

2. на внутрішньодержавному рівні – з іншими правоохоронними органами України, трудовими колективами, громадськими організаціями та населенням;

3. на міжнародному рівні – з правоохоронними органами інших країн. Основними формами співробітництва правоохоронних органів України з правоохоронними органами інших країн є:

– обмін оперативною інформацією;

– надання правової допомоги в кримінальних справах;

– виїзд членів слідчо-оперативних груп за кордон для участі у слідчих діях та оперативних заходах;

– виїзд для обміну оперативною інформацією;

– виїзд за кордон для участі у слідчих та інших діях у рамках надання правової допомоги;

– виїзд для супроводу розшукуваних та затриманих осіб за кордоном;

– виїзд працівників прикордонних управлінь та управлінь внутрішніх справ України в прилеглі регіони сусідніх країн у рамках оперативних справ;

– прибуття працівників правоохоронних органів іноземних країн в Україну для здійснення слідчих та оперативних заходів;

Підводячи підсумки, зазначимо, що сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального

інформаційного простору. Саме тому ми маємо використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки [189, с. 225].

Оскільки створення інформаційного суспільства є невід'ємною складовою, важливо не тільки розширювати можливості технологічного обміну інформацією, але й глибоко усвідомлювати всіма учасниками інформаційних відносин – власниками, користувачами та виробниками інформаційних технологій, агентами постачання послуг, а також державою – необхідність захисту інформаційних ресурсів та забезпечення національної безпеки. Це також включає врахування міжнародного досвіду боротьби зі злочинністю у сфері інформаційних технологій у сфері правового забезпечення.

Лише через спільні зусилля організацій і відомств незалежно від форм власності та налагодження міжнародного співробітництва, використовуючи сучасні технології захисту інформації, можна досягти переваг не лише у сфері електронного бізнесу, а й у загальній інформаційній революції, забезпечивши при цьому інформаційну безпеку держави та її громадян. Важливо наголосити, що удосконалення правового забезпечення протидії злочинності у сфері інформаційних технологій в Україні має відбуватися з урахуванням національних культурно-історичних та соціально-економічних особливостей країни, базуючись на детальному аналізі міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю, з метою оптимального впровадження в європейське та світове правове поле [198].

Отже, в сучасний момент Україні важливо фокусуватися на двох основних спрямуваннях:

– розглядати український внутрішній простір як сучасний, повноцінний та конкурентоспроможний.

– гарантувати активну присутність держави в світі та підтримувати позитивний її імідж.

– забезпечення національної безпеки має відбуватися з врахуванням пріоритетності національних інтересів та вчасного вжиття адекватних заходів, відповідних характеру та масштабам загроз для цих інтересів. Це повинно ґрунтуватися на принципах правової демократичної держави. Оскільки інформаційна безпека є невід'ємною складовою національної безпеки, у цій сфері також слід надавати пріоритет національним інтересам.

Таким чином, ключовими напрямами державної політики з питань національної безпеки України в інформаційній сфері є:

– гарантування незалежності інформаційної сфери України;

– удосконалення державного регулювання розвитку інформаційної галузі через створення правових та економічних умов для розвитку національної інформаційної інфраструктури та ресурсів, використання передових технологій, заповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до запобігання та протидії корупції, зловживанням службовим становищем та іншим явищам, що становлять загрозу національній безпеці України. Також гарантування поваги конституційних прав на свободу слова, доступ до інформації, захист персональних даних, запобігання незаконному втручанню в діяльність ЗМІ та журналістів, заборона цензури, дискримінації в інформаційній сфері та переслідування журналістів за політичні переконання, виконання професійних обов'язків та критику;

– проведення комплексу заходів для захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Удосконалення правового забезпечення в сфері протидії запобігання злочинності у сфері інформаційних технологій можливе через вжиття таких заходів:

– внесення змін до Кримінального кодексу України, спрямованих на посилення відповідальності за кримінальні правопорушення у сфері комп'ютерних та інформаційних технологій.

– визнання електронних документів та інших даних як доказової бази при розслідуванні кіберзлочинів.

– чітка регламентація механізмів взаємодії між клієнтом та банком, а також між банками відправника та отримувача коштів у разі несанкціонованого списання коштів з рахунку клієнта, шляхом змін до Інструкції про безготівкові розрахунки в Україні в національній валюті.

– введення практики ідентифікації користувача Інтернету через надання ідентифікаційного коду особи оператору зв'язку при укладенні договору на надання послуг.

– установлення вимоги щодо обов'язкового проведення двоканальної аутентифікації та негайного онлайн-інформування клієнтів про кожну проведену операцію.

– накладення обов'язку на банки надавати безоплатно послугу СМС-інформування про будь-які операції за поточними картковими рахунками.

– встановлення вимоги для банків здійснювати вихідні платежі клієнтів лише з наявних коштів на їх рахунках на початок операційного дня. Це надасть банку та постраждалому клієнту можливість заблокувати кошти на рахунку недобросовісного отримувача в разі несанкціонованого списання коштів.

– впровадження процедури сертифікації електронних платіжних засобів.

– визначення фіксованого максимального обсягу видачі готівки, який може здійснюватись в позаопераційний час банку через банкомат по одному картковому рахунку та невідкладна необхідність узгодження цього обсягу.

– впровадження вимоги для банків обладнувати всі банкомати антискімінговими пристроями.

– введення обов'язку для банків реєстрації Інтернет-магазинів в податкових органах щодо конкретних платників податків.

Висновки до Розділу 4

1. У нашій країні кількість правопорушень у сфері інформаційних технологій не є значною у порівнянні з країнами, такими як США, Великобританія, Німеччина та інші, де відбуваються надзвичайно великі масштаби таких порушень. Однак існує тенденція до зростання цього виду злочинності, що підтверджують статистичні дані.

Порівняльно-правовий аналіз законодавства цих країн і України свідчить про те, що за кордоном у більшості держав створена комплексна система органів для забезпечення кібербезпеки. Наприклад, у США існує Управління національної безпеки (Department of Homeland Security), в межах якого працює спеціальний кібербезпековий департамент, що відповідає за безпеку високотехнологічних систем країни. Також існує Кіберкомандування, яке веде спеціальні підрозділи з метою розвідування мереж, захисту

власних мереж, блокування та дезорганізації структур супротивника в кіберпросторі.

2. Відзначено, що криміналізація дій, які утворюють злочинність у сфері інформаційних технологій, є окремою науковою та практичною проблемою, яка може бути вирішена лише через розробку універсальної концепції кіберзлочинності та уніфікацію норм міжнародного права.

Отже, у сфері регулювання злочинності у сфері інформаційних технологій відсутній консенсус та єдність в міжнародному правовому вимірі. Це невід'ємно призводить до зменшення ефективності контролю та сприяє виникненню конфліктів і прогалин. В той самий час швидкі технологічні просування відбуваються настільки стрімко, що ця проблема у майбутньому стане ще більш актуальною.

3. У сучасний час Україні особливо важливо забезпечити інформаційну безпеку, що стосується як численних атак на національний інформаційний простір з боку інших країн і їх контрольованих суб'єктів, так і активізації процесів євроінтеграції України та участі держави в міжнародних безпекових заходах та програмах, які підтримуються Сполученими Штатами Америки та іншими країнами.

Для України перехід до нового етапу суспільного розвитку означає невід'ємну ситуацію, в якій поліпшення організації використання інформаційної основи для розвитку української нації і держави – це об'єднана система вітчизняних інформаційних баз, а також розвиток інформаційного виробництва та систем соціальних інформаційних комунікацій, що у сукупності утворюють ресурсну базу вітчизняного інформаційного простору, – може гарантувати належні позиції в міжнародному співробітництві.

ВИСНОВКИ

У висновках сформульовано найбільш суттєві положення, отримані у результаті монографічного дослідження, наведено нове вирішення наукової проблеми щодо дослідження теоретико-прикладних засад запобігання злочинності у сфері інформаційних технологій, а також науково обґрунтовані рекомендації та пропозиції щодо вдосконалення правової регламентації і практики такої діяльності:

1. Висвітлено стан наукової розробленості запобігання злочинності у сфері інформаційних технологій. На основі вивчення наукових джерел щодо забезпечення інформаційної безпеки в Україні та запобігання злочинності у цій сфері виокремлено напрями наукових досліджень: 1) дослідження загальних засад інформаційної безпеки в Україні (В. А. Ліпкан, В. А. Залізняк, Ю. Є. Максименко, В. М. Желіховський, В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк, А. В. Тунік, Д. В. Дубов); 2) вивчення правового забезпечення інформаційної безпеки в Україні (І. С. Стаценко-Сургучова, І. Р. Березовська, Т. В. Скубіна); 3) безпекові дослідження (О. М. Яхно); 4) загально-правові питання забезпечення кібербезпеки (Є. Я. Прохоренко, О. О. Проскурін, Н. Б. Новицька, А. М. Коломієць); 5) теоретичні аспекти кримінологічної характеристики кіберзлочинності (Ш. Шольберг, Д. Паркер, С. Хантінгтон, О. В. Таволжанський, Н. В. Сметаніна, М. В. Карчевський, В. В. Пивоваров, В. А. Номоконов та Т. Л. Тропіна, В. М. Бутузов, С. А. Буяджи, Г. М. Чернишов, М. О. Кравцова, О. Е. Радутний, С. В. Шапочка); 6) криміналістичні аспекти розслідування (В. М. Шевчук та В. Ю. Шепітько, В. С. Бабійчук).

2. Досліджено генезу та історичний розвиток запобігання злочинності у сфері інформаційних технологій. Встановлено, що основними рисами початку розвитку кіберзлочинності є: 1) перші випадки кримінальних правопорушень, вчинених з використанням електронних обчислювальних машин, свідчать про початок цього явища та зростання інтересу до комп'ютерної та мережевої діяльності як засобу для вчинення кримінальних правопорушень; 2) формування організованих злочинних груп, які використовували свої знання для незаконного збагачення та порушення встановленого порядку, свідчить про еволюцію цього явища від окремих випадків

до організованої діяльності; 3) на цьому етапі відсутність ефективних інструментів правового регулювання боротьби з кіберзлочинністю стала значущим обмеженням у протидії цим кримінальним правопорушенням; 4) також варто відзначити, що на тому етапі існувала відсутність випадків покарання комп'ютерних злочинців за їх протиправну діяльність, оскільки правова база для цього була недостатньо розвиненою.

3. Розглянуто методологію кримінологічного дослідження злочинності у сфері інформаційних технологій. Злочинність у сфері інформаційних технологій і її запобігання у її поєднанні динамізму та статичності, мінливість, структурованість, багатоплановість зумовлюють і відповідну структуру методології її дослідження, що складається з таких складових частин: домінуючого світогляду, типу наукового мислення, філософських засад, наукових парадигм, методологічних підходів та наукових методів.

До основних аспектів методології дослідження злочинності у сфері інформаційних технологій віднесено: 1) мультидисциплінарний підхід: дослідження злочинності у сфері інформаційних технологій вимагає співпраці між різними галузями науки та індустрією, включаючи правознавців, комп'ютерних фахівців, психологів, соціологів і багатьох інших. Мультидисциплінарний підхід дозволяє більш повно розуміти і аналізувати злочинність у сфері інформаційних технологій; 2) вивчення технологій: зростання злочинності у сфері інформаційних технологій часто пов'язане з використанням новітніх технологій. Дослідники повинні слідкувати за останніми розвитками у сфері інформаційних технологій та кібербезпеки; 3) збір та аналіз даних: збір і аналіз великих обсягів даних може допомогти виявити патерни та тренди в кіберзлочинності. Методи аналізу даних, такі як машинне навчання і аналіз великих даних, стають все більш важливими в цій галузі; 4) етичні аспекти: врахування етичних аспектів дослідження злочинності у сфері інформаційних технологій, таких як приватність і безпека даних, також має велике значення; 5) правова складова: аналіз правового регулювання і кримінального переслідування злочинності у сфері інформаційних технологій є важливою складовою дослідження; 6) соціальні аспекти: розуміння соціальних аспектів злочинності у сфері інформаційних технологій, включаючи мотиви та наслідки кіберзлочинців, також є важливим; 7) методи попередження і реагування: розробка методів та стратегій для попередження та реагування на злочинність у сфері

інформаційних технологій також є важливою частиною дослідження.

4. Зроблено висновок, що створення ефективної системи координації та взаємодії між органами державної влади України у сфері стратегічних комунікацій є критично важливим для забезпечення ефективного захисту національного інформаційного простору та національної безпеки. Для досягнення цього запропоновано впровадити декілька можливих кроків: 1) створення центрального координаційного органу: уряд України може створити центральний орган або комітет, відповідальний за координацію інформаційних зусиль у сфері стратегічних комунікацій. Цей орган може об'єднувати представників різних міністерств та агентств для забезпечення єдиної стратегії та координації дій. 2) розробка стратегії інформаційної безпеки: Україна повинна розробити оновлену національну стратегію інформаційної безпеки, яка визначатиме загальні цілі та пріоритети в цій сфері. Ця стратегія має враховувати внутрішні та зовнішні загрози та визначати конкретні заходи для їх протидії. 3) створення механізмів обміну інформацією: важливо встановити механізми обміну інформацією між різними органами та агентствами, які займаються інформаційною безпекою. Це допоможе у вчасному реагуванні на загрози та координації заходів. 4) підвищення інформаційної грамотності: уряд може запровадити програми для підвищення інформаційної грамотності серед населення, що допоможе громадянам відрізняти правдиву інформацію від дезінформації та фейкових новин. 5) захист інформаційної інфраструктури: для забезпечення захисту національної інформаційної інфраструктури важливо розглянути введення сучасних технологій та кіберзахисту. 6) співпраця з міжнародними партнерами: Україна може співпрацювати з міжнародними організаціями та партнерами для обміну досвідом та інформацією щодо інформаційної безпеки.

5. Проаналізовано якісні та кількісні показники злочинності у сфері інформаційних технологій в Україні. Доведено, що аналіз рівня кіберзлочинності протягом 2020–2022 років не дає повної картини стосовно цього явища, оскільки злочинність у сфері інформаційних технологій характеризується значним рівнем таємничості. Деякі ознаки цієї таємничості включають негативну реакцію потенційних жертв кіберзлочинів або свідків, недоліки у роботі

правоохоронних органів у відповідь на повідомлення про кіберзлочини, та високий технологічний рівень здійснення кіберзлочинів, який охоплює різні сфери життя. Ці фактори таємничості підкреслюють серйозну загрозу злочинності у сфері інформаційних технологій для суспільства, оскільки надають нові можливості кримінальному світові у віртуальному просторі. Для більш точного вивчення поточного стану кіберзлочинності можна проаналізовано зміну коефіцієнтів кримінальних правопорушень у сфері інформаційних технологій на кожних 100 тисяч населення загалом.

Рівень кіберзлочинності був найнижчим у 2020 році (5,9), а найвищим у 2022 році, коли він склав 8,3. З цих результатів очевидно, що коефіцієнт кіберзлочинності у 2022 році збільшився на 5 % порівняно з 2021 роком. Крім того, спостерігається значний зріст коефіцієнта кіберзлочинності з початку досліджуваного періоду до 2022 року. Отже, аналізуючи зміни в структурі кіберзлочинності протягом 2020–2022 років, виявлено дві основні тенденції: негативна та позитивна. Негативна тенденція виявляється у зростанні кількості кримінальних порушень, передбачених статтями 361-1 та 362 КК України, в той час як позитивна тенденція проявляється у зменшенні кількості зареєстрованих кримінальних правопорушень, передбачених статтями 361 та 361-2 КК України.

6. Запропоновано авторське визначення кримінальних правопорушень у сфері інформаційних технологій, під якими варто розуміти кримінально протиправні діяння (дія або бездіяльність), які посягають на права та свободи осіб, держави шляхом використання таким чином, порушуючи інформаційну безпеку, задля матеріальної чи особистої вигоди.

Зазначено, що поняття «кіберзлочини» та «комп'ютерні злочини» – це різні поняття. «Кіберзлочинність» більш ширше поняття, а «комп'ютерні злочини» – вужче поняття, яке передбачає використання лише комп'ютерної техніки під час вчинення даних кримінальних правопорушень або коли комп'ютерна техніка, або інформація, яка міститься на ній є предметом даного кримінального правопорушення. А якщо говорити про «кіберзлочини», то тут уже потрібно розглядати ширше коло застосовуваних злочинцями технічних пристроїв, які працюють по типу комп'ютерів, але таким не є.

Виокремлено групи мотивів вчинення кіберзлочинів:

– раціональні мотиви (сюди можуть входити корисливі, політичні мотиви, релігійні мотиви);

– емоційні мотиви (мотив помсти, мотив гри);

– моральні мотиви (хуліганські мотиви, мотив справедливості);

– змішані мотиви (дуже часто поєднуються емоційні з моральними мотивами).

7. Представлено авторську класифікацію осіб, що вчиняють кримінальні правопорушення у сфері інформаційних технологій:
1) кримінальні правопорушення, що порушують доступність, конфіденційність та цілісність комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в систему та дані);
2) кримінальні правопорушення, пов'язані з використанням комп'ютера як інструмента для вчинення кримінальних правопорушень (маніпуляції з інформацією), такі як комп'ютерне підроблення та комп'ютерне шахрайство; 3) кримінальні правопорушення, пов'язані з контентом, зокрема з вмістом даних у комп'ютерних мережах (особливо розповсюджені кримінальні правопорушення, пов'язані з дитячою порнографією); 4) порушення авторського права і суміжних прав (визнання порушень, пов'язаних з авторським правом, компетенцією національних законодавств країн); 5) акти расизму та ксенофобії, вчинених за допомогою комп'ютерних мереж; 6) кібертероризм (кібервійни).

8. Виокремлено основні підходи щодо запобігання діянь, пов'язаних з кіберзагрозами, і розглядати кібербезпеку як пріоритетну сферу національної безпеки: 1) Законодавство та стратегії: прийняття Закону про кібернетичну безпеку та розробка національної стратегії кібербезпеки є ключовими кроками. Ці документи нададуть важливий законодавчий та стратегічний каркас для боротьби з кіберзагрозами.
2) Охорона інтелектуальної власності: Захист інтелектуальної власності є критично важливим в контексті кібербезпеки, оскільки багато атак спрямовані на витіснення конфіденційної інформації та інтелектуальних активів. Важливо розвивати засоби захисту цінної інформації. 3) Навчання і підготовка: внесення змін до навчальних програм та навчальних планів, що стосуються кібербезпеки, є ключовим для підготовки нового покоління фахівців у цій галузі. Забезпечення підготовки фахівців у галузі кібербезпеки допоможе розвивати кадровий потенціал країни. 4) Міжнародна співпраця: Кіберзагрози часто транснаціональні, і співпраця на міжнародному рівні є ключем до їхнього вирішення. Україна може брати активну участь у міжнародних ініціативах та навчаннях з кібербезпеки, що сприятиме обміну досвідом та спільній боротьбі з кіберзагрозами.

5) Свідомість і готовність громадськості: Важливо підвищувати свідомість громадськості щодо кібербезпеки і пропагувати культуру безпеки в інтернеті. Це може включати в себе навчальні програми для громадян і важливість звітування про кіберзагрози.

9. Розглянуто нормативно-правове забезпечення запобігання злочинності у сфері інформаційних технологій. Доведено, що поряд з нормативно-правовим забезпеченням, заходи боротьби з кіберзлочинністю повинні також супроводжуватися середньостроковими і довгостроковими стратегічними концепціями, спрямованими на захист інформаційних ресурсів і притягнення розробників кримінально протиправних схем до відповідальності.

Важливими аспектами такого підходу є: 1) стратегічний кіберзахист: Розвиток стратегічних цілей і політики кіберзахисту допомагає визначити пріоритети та напрямки для зміцнення кібербезпеки країни. Це може включати в себе розробку національних стратегій кіберзахисту і створення центральних органів для координації цих зусиль; 2) усвідомлення загроз: Важливо постійно аналізувати нові кіберзагрози та визначати їхні наслідки для національної безпеки; 3) розвиток кадрів: Навчання і розвиток кадрів у галузі кіберзахисту є ключовим аспектом. Потрібно створювати програми навчання та підготовки, які допоможуть забезпечити наявність кваліфікованих фахівців; 4) міжнародне співробітництво: Боротьба з кіберзлочинністю вимагає співпраці з іншими країнами і міжнародними організаціями. Укладання міжнародних договорів та обмін інформацією є важливими аспектами цієї співпраці; 5) профілактика та свідомість громадськості: Важливо надавати інформацію громадськості та бізнесу щодо кіберзагроз і заходів для їх попередження; 6) кримінальна відповідальність: Законодавство повинно передбачати кримінальну відповідальність для кіберзлочинців і забезпечувати їхнє притягнення до відповідальності.

10. Надано характеристику суб’єктів запобігання злочинності у сфері інформаційних технологій в Україні. Доведено, що держава повинна приділяти більше уваги запобіганню кіберзлочинності через адекватне фінансування та технічне забезпечення відповідних органів. Крім того, може бути доцільним перегляд організаційної структури боротьби з кіберзлочинами, наприклад, створення єдиного централізованого органу, що підпорядковується виконавчій владі. Такий орган може відігравати ключову роль в запобіганні та боротьбі з кіберзлочинністю в Україні.

11. Доведено необхідність впровадження відповідальності за вищезазначені кримінальні правопорушення, вчинені під час воєнного стану. За такі протиправні дії повинні передбачатися суворі санкції, оскільки обставини в країні вимагають цього. Особа, яка завдає шкоди національним інтересам України у кіберпросторі і таким чином допомагає агресору в цій війні, повинна нести відповідальність, аналогічно воєнним злочинцям.

12. Підсумовано, що необхідність впровадження ефективних заходів протидії сучасним загрозам інформаційній безпеці, зокрема кіберзагрозам, вимагає удосконалення форм і методів захисту інформації, критичної інформаційної інфраструктури та інформаційно-психологічної безпеки громадян. Цей підхід практикують у всіх європейських країнах. Україна, обравши курс на євроінтеграцію, повинна орієнтуватися на стратегію розвитку країн-учасниць Європейського Союзу в сфері інформації.

13. Виокремлено напрями удосконалення правового забезпечення в сфері запобігання злочинності у сфері інформаційних технологій: внесення змін до Кримінального кодексу України, спрямованих на посилення відповідальності за кримінальні правопорушення у сфері комп'ютерних та інформаційних технологій; визнання електронних документів та інших даних як доказової бази при розслідуванні кіберзлочинів; чітка регламентація механізмів взаємодії між клієнтом та банком, а також між банками відправника та отримувача коштів у разі несанкціонованого списання коштів з рахунку клієнта, шляхом змін до Інструкції про безготівкові розрахунки в Україні в національній валюті; введення практики ідентифікації користувача Інтернету через надання ідентифікаційного коду особи оператору зв'язку при укладенні договору на надання послуг; установлення вимоги щодо обов'язкового проведення двоканальної аутентифікації та негайного онлайн-інформування клієнтів про кожну проведену операцію; накладення обов'язку на банки надавати безоплатно послугу СМС-інформування про будь-які операції за поточними картковими рахунками; встановлення вимоги для банків здійснювати вихідні платежі клієнтів лише з наявних коштів на їх рахунках на початок операційного дня. Це надасть банку та постраждалому клієнту можливість заблокувати кошти на рахунку недобросовісного

отримувача в разі несанкціонованого списання коштів; впровадження процедури сертифікації електронних платіжних засобів тощо.

14. На основі позитивного досвіду зарубіжних країн сформовано модель забезпечення інформаційної безпеки в мережі internet, яка повинна базуватись на цілісній і розгалуженій системі державних органів і неурядових організацій, діяльність яких спрямована на запобіганні злочинності у сфері інформаційних технологій. Така модель повинна бути реалізована на двох рівнях: 1) рівень наукового аналізу, який досліджуватиме ризики кібербезпеки відповідно до можливих кіберзагроз та наслідків, актуалізуватиме засоби та методи забезпечення кібербезпеки. Це є одним із найважливіших завдань. Оскільки проблема полягає в складності класифікації загроз, що виходять як з території держави, так і виникають безпосередньо в межах держави, важливо наголосити на необхідності для будь-якої держави розробити стратегію ідентифікації кіберзагроз, а також їх вчасного виявлення, запобігання, захисту та мінімізації наслідків; 2) виконавчий рівень, що координуватиме дії в двох напрямках: внутрішньому (між національними структурами, відповідальними за виявлення та протидію кіберзагрозам) та зовнішньому, коли координація здійснюється між національними структурами та аналогічними міжнародними організаціями.

15. Запобігання злочинності у сфері інформаційних технологій та потреба у міжнародному співробітництві в цьому контексті вимагає створення міжнародних процедур надання допомоги під час розслідування таких кримінальних правопорушень та утворення координаційних органів в межах міжнародних правоохоронних установ, таких як ООН, Інтерпол, Рада Європи та інші.

Задля впровадження міжнародно-правового законодавства щодо запобігання злочинності у сфері інформаційних технологій, необхідно здійснити такі кроки: впровадження часткового розкриття даних про рух інформації як складової частини термінового збереження даних; об’єднання у одному заході забезпечення – збереження цифрових даних, як термінове збереження та часткове розкриття даних (статті 16, 17 Конвенції про кіберзлочинність), так і арешту цифрових даних після отримання до них доступу (пункт 3 статті 19 Конвенції) – для збереження цифрового оригіналу; встановлення кримінальної відповідальності за порушення збереження чи розкриття даних: а) передбачення кримінальної, а не адміністративної відповідальності; б) розширення відповідальності не тільки на фізичних осіб, але й на юридичних осіб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Абакумов В. М. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони. *Форум права*. 2012. No 4. С. 10–16.
2. Абламський С.Є. Особливості здійснення тимчасового доступу до електронних інформаційних систем або їх частин, мобільних терміналів систем зв’язку. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2017. № 2(78). С. 239–245. URL: https://journal.lduvs.lg.ua/index.php/journal/article/view/305.
3. Азаров Д. Порушення роботи автоматизованих систем – злочини у сфері комп’ютерної інформації. *Право України*. 2000. № 12. С. 69–73.
4. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп’ютерної інформації : дис. … канд. юрид. наук : 12.00.08 / НАНУ. Інститут держави і права ім. В. М. Корецького. Київ, 2002. 228 с.
5. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали Міжнародної науково практичної конференції. За ред. О. В. Манжай. Харків, 2014. МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.
6. Александров Ю. В., Біленчук П. Д., Валлє В. О., Гель А. П., Ковальський В. С., Костенко О. М., Перелигіна Р. В., Семаков Г. С. Кримінологія: підручник. Практикум. Київ: Юрінком Інтер, 2017. 344 с.
7. Алієв М. М., Куньо А. М. Проблема кіберзлочинності та шляхи її подолання у сучасному інформаційному суспільстві. XI Міжнародна науково-технічна конференція «*АВІА-2013*», 21–23 травня 2013 р. К.: НАУ, 2013. Т.6. С. 35–38.
8. Амелін О. Злочини у сфері інформаційних відносин в міжнародно-правових актах. *Науковий часопис Національної академії прокуратури України.* 2016. № 2. С. 5
9. Андрійчук М. Т., Андрійчук Т. С. Взаємодія мас-медіа та органів державної влади: навч. посіб. КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2018. 114 с.

10. Аніщук В. В. Інформаційна безпека як об’єкт посягання злочинів проти основ національної безпеки України. *Науковий вісник Ужгородського національного університету*. 2023. С. 139–143.
11. Ансельмо Е. Кіберпростір у міжнародному законодавстві: чи спростовує розвиток Інтернету принцип територіальності у міжнародному праві? *Економічні стратегії*. 2006. № 2. С. 24–31.
12. Антонюк В. В. Основні науково-методологічні підходи до дослідження державної політики інформаційної безпеки. *Інвестиції: практика та досвід.* 2013. № 20. С. 143–147.
13. Архипова Є. О. Соціально-філософське осмислення поняття «інформаційна безпека». *Вісник Нац. технічного ун-ту України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка.* 2011. № 3. С. 7–11.
14. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. К.: ВПЦ «Київський університет», 2018. 229 с.
15. Бабійчук В. С. Кібертероризм та протидія йому. *Young Scientist*. 2019. No 4 (68). С. 103–107.
16. Бараненко Р. В. Кіберзлочин, комп’ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2021. Випуск 1 (49). С. 80–87.
17. Барометр свободи слова за серпень 2014 р. Інститут масової інформації, 2014. URL: http://imi.org.ua/barametr/45643-barometr-svobodi-slova-za- serpen-2014-roku.html.
18. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414–418
19. Березовська І. Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2012. 18 с.
20. Берназ В. Д., Бірюков В. В., Волобуєв А.Ф. Криміналістика: підручник. Х.: ХНУВС, 2011. 666 с.
21. Бєлкін Л. М., Юринець Ю. Л., Бєлкін М. Л., Криволап Є. В. Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України. *Юридичний вісник*. 2022. № 3 (64). С. 78–86. DOI: https://doi.org/10.18372/2307-9061.64.16893.

22. Біла І. О. Сучасний стан кримінальної злочинності в галузі інформаційних технологій. URL: http://dspace.onu.edu.ua:8080/bitstream/123456789/24461/1/101-105.pdf
23. Біленчук Д. П. Кібрешахраї – хто вони? *Міліція України.* 1999. № 7–8. С. 32–34.
24. Біленчук П. Д. Конвергенція квантового майбутнього: правове, освітнє, наукове і ресурсне забезпечення. *Юридичний вісник України*. 2018. № 42–43. С. 16–17.
25. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: навч. посіб. К.: Українська академія внутрішніх справ, 1994. 72 с.
26. Біленчук П. Д., Малій М. І. Криміналістичне та судово-експертне забезпечення розвитку квантового майбутнього в третьому тисячолітті. *Актуальні проблеми криміналістики та судової експертології*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 22 листопада 2018р.). Редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ: НАВС, 2018. С. 57–62.
27. Білобров Т. В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України: дис. … канд. юрид. наук. Київ, 2020. 209 с.
28. Білобров Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 96–102. URL: http://pravoisuspilstvo.org.ua/archive/2020/3_2020/20.pdf.
29. Бобришева О. Інформаційна безпека бібліотеки: проблеми та шляхи формування. *Вісник Книжкової палати*. 2010. No 12. С. 18–20.
30. Бодунова О. The need for interaction between the media and law enforcement agencies under martial law in Ukraine. Матеріали Міжнародної науково-практичної конференції «*Реформування кримінального провадження в Україні: кримінальні процесуальні та криміналістичні аспекти*» (м. Ірпінь, 20 травня 2022 р.). С. 229–233.
31. Бодунова О. М. Criminology principles of digitalization of state structures: global experience. *Соціологія права*. 2022. Випуск 1–2 (40–41). С. 7–10. http://soclaw.idpnan.kyiv.ua/archive/2022/1–2/1.pdf.
32. Бодунова О. М. The use of information technology in the commission of criminal offenses under martial law in Ukraine. Матеріали Міжнародної науково-практичної конференції

«Міжнародне право XXI століття: сучасність та майбутнє», м. Ірпінь (25 травня 2022 року). С. 34–38.
33. Бодунова О. М. Взаємодія засобів масової інформації з правоохоронними органами України в запобіганні злочинності. *Вісник Вищої кваліфікаційної комісії суддів України.* 2019. № 2. С. 46–54.
34. Бодунова О. М. Діджиталізація як напрям запобігання злочинності у сфері інформаційних технологій. Матеріали Міжнародної науково-практичної конференції «*Міжнародно-правова оцінка російської воєнної агресії в Україні та захист фундаментальних прав людини*», м. Київ. 16 липня 2022. С. 291–293.
35. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій: міжнародно-правовий аспект. *Електронне наукове фахове видання «Юридичний науковий електронний журнал».* 2020. №4. С. 246–249.
36. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського національного університету.* 2023. № 75. Т. 2. С. 83–87. http://visnyk-pravo.uzhnu.edu.ua/article/view/276140.
37. Бодунова О. М. Запобігання кібершахрайству у фінансовому секторі. *Ірпінський юридичний часопис*. 2023. № 3 (12). С. 194–200. URL: https://drive.google.com/file/d/1wJrT-86XsnozaO4W8ST8kYM8JO ZFWMqK/view.
38. Бодунова О. М. Інформатизація суспільства як детермінант податкової злочинності. *«Права людини та проблеми організації і функціонування публічної адміністрації в умовах становлення громадянського суспільства в Україні»*: матеріали Міжнародної науково-практичної конференції, 23–24 квітня 2021 року. Запоріжжя : Запорізька міська громадська організація «Істина», 2021. С. 82–84.
39. Бодунова О. М. Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. *Аналітично-порівняльне законодавство*. 2023. №1. С. 441–446. http://app-journal.in.ua/wp-content/uploads/2023/04/APP_01_2023_FINAL.pdf.
40. Бодунова О. М. Кіберзлочинність в умовах воєнного стану: деякі особливості запобігання. Матеріали Міжнародної-науково-практичної конференції *«Стан кримінально-правового забезпечення в Україні»,* 31 березня 2023 року. С. 61–65.

41. Бодунова О. М. Кримінально-правові засади забезпечення кібербезпеки в Україні. Матеріали Міжнародної науково-практичної конференції «*Вплив інтеграційних тенденцій та розвиток національного права*», Одеса, 25 лютого 2022 р. С. 45–47.
42. Бодунова О. М. Кримінологічна характеристика особи, що вчиняє кримінальні правопорушення у сфері інформаційних технологій. *Ірпінський юридичний часопис*. 2022. №1. С. 151–159.
43. Бодунова О. М. Міжнародно-правова протидія злочинності у сфері інформаційних технологій. Тези доповідей Міжнародної науково-практичної інтернет-конференції *«Сучасний стан кримінального законодавства України: шляхи реформування»*, м. Ірпінь, 1 березня 2018 року. С. 39–42.
44. Бодунова О. М. Окремі напрями запобігання корупційної злочинності в Україні в умовах цифровізації державних структур. Матеріали V Всеукраїнської науково-практичної конференції *«Наукові розвідки з актуальних проблем публічного та приватного права»,* м. Київ, (20 травня 2022 р.). Київський університет імені Бориса Грінченка. С. 34–36.
45. Бодунова О. М. Окремі напрями покращення взаємодії ЗМІ із правоохоронними органами у запобіганні злочинності в інформаційній сфері. *Юридична наука*. 2020. № 2(104). С. 5–11.
46. Бодунова О. М. Посилення відповідальності за кримінальні правопорушення у сфері інформаційних технологій: виклики сьогодення. Матеріали Всеукраїнській науково-практичній конференції «*Актуальні питання та перспективи розвитку кримінального права, кримінології та судочинства*», присвяченої 275-річниці з дня народження Джеремі Бентама, 12 травня 2023 року, м. Київ. С. 16–19.
47. Бодунова О. М. Сучасний стан запобігання злочинності у сфері інформаційних технологій. Збірник матеріалів «IV Всеукраїнських науково-правових читаннях» пам’яті доктора юридичних наук, професора, Заслуженого юриста України, член-кореспондента Національної академії правових наук України Ніни Романівни Нижник. за заг. ред. А. Є. Шевченка. Вінниця: ТОВ «ТВОРИ», 2020. С. 85–88.
48. Бодунова О. М. Сучасний стан злочинності у сфері інформаційних технологій. Матеріали Міжнародної науково-практичної конференції до Дня науки *«Актуальні проблеми*

національної правової реформи». 17 травня 2021 р., Київ, Академія адвокатури України. С. 71–73.
49. Бодунова О. М. Теоретико-правові засади визначення поняття злочинів у сфері інформаційних технологій. *Вісник Вищої кваліфікаційної комісії суддів України.* 2019. № 3. С. 17–21.
50. Бодунова О. М. Щодо необхідності розширення системи кримінальних правопорушень у сфері інформаційних технологій. Матеріали XIII Міжнародної науково-практичної конференції *«Свобода, безпека та незалежність: правовий вимір»,* м. Київ, 24 лютого 2023 року. С. 314–315.
51. Бодунова О. М., Бусол О. Ю. та інші. Законодавче забезпечення протидії корупції: навчальний посібника. За заг. редакцією В.В. Топчія. Вінниця : Твори, 2021. 216 с.
52. Бодунова О. М., Гасимов З. Правові аспекти боротьби з кібершахрайством в Україні. Матеріали IV Міжнародної науково-практичної конференції *«Фінансова політика: теоретичні та практичні аспекти юридичної науки»,* 7 квітня 2021 року, м. Ірпінь. С. 246–249.
53. Бодунова О. М., Гасимов З. Правові аспекти боротьби з кібершахрайством в Україні. Матеріали IV Міжнародної науково-практичної конференції «Фінансова політика: теоретичні та практичні аспекти юридичної науки», м. Ірпінь, 7 квітня 2021 року. С. 253–255.
54. Бодунова О. М., Гасимов З. Соціальні мережі як засіб вчинення кримінальних правопорушень у сфері інформаційних технологій. Збірник тез доповідей Міжнародної науково-практичної інтернет-конференції *«Сучасний стан кримінально-правового забезпечення в Україні»*, м. Ірпінь, 5 березня 2021 року. С. 16–21.
55. Бодунова О. М., Дідківська Г. В., Нікітін Ю. В. та інші Кримінальне право України. Особлива частина. Навчальний посібник. За заг. ред. В. В. Топчія. Вінниця : Твори, 2021. 412 с.
56. Бодунова О. М., Лямзіна О. В. Цифровізація органів державної влади як захід запобігання корупційної злочинності в Україні. *Наукове фахове видання «Актуальні проблеми вдосконалення чинного законодавства України».* 2022. № 58. С. 27–36.
57. Бодунова О. М., Топчій В. В. Нормативно-правові засади цифровізації сфери надання адміністративних послуг. *Юридична наука*. 2020. № 9. С. 178–184. URL: https://legal.nam.edu.ua/archives/

58. Бодунова О. М., Топчій В. В. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис*. 2023. № 1(10). С. 187–195.
59. Бодунова О. М., Топчій В. В. Цифрова трансформація як об'єкт публічного адміністрування. *Науковий вісник публічного та приватного права*. 2021. Випуск 4. Том 2. С. 114–118. URL: http://www.nvppp.in.ua/vip/2021/2-2/10.pdf.
60. Бодунова О. М., Топчій В. В., Дідківська Г. В. та ін. Кримінологічні засади участі України у міжнародній системі запобігання злочинності: монографія: / Вінниця, ТОВ «ТВОРИ». 2021, 376 с.
61. Бодунова О. М., Яцик Т. П. Розповсюдження фейкової інформації як загроза інформаційній безпеці України. Матеріали Міжвідомчого круглого столу *«Протидія фейкам в Україні як складова інформаційної безпеки держави»,* 20 травня 2021 року, м. Київ. С. 119–122.
62. Бодунова О. М., Яцик Т. П. Роль засобів масової інформації у запобіганні злочинності в інформаційній сфері. *Науковий юридичний журнал «Правові новели».* 2020. № 10. Том ІІІ. С. 117–122.
63. Бодунова О. М., Яцик Т. П. Щодо розмежування понять «інформаційна безпека» та «кібербезпека». *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція».* 2020. Випуск 47. Том 2. С. 64–66.
64. Бодунова О. Співпраця ЗМІ з правоохоронними органами в умовах воєнного стану. Матеріали Міжнародного конгресу *«Фінанси, економіка vs війна»,* м. Ірпінь, 27 квітня 2022 р. С. 737–741.
65. Бодунова О.М., Любавіна В.П. Вплив новітніх технологій на динаміку злочинності в Україні. *Право і суспільство*. 2018. № 4. С. 225–229.
66. Бодунова О.М., Топчій В.В. Адміністративно-правове забезпечення цифровізації органів державної влади як напряму запобігання корупційної правопорушень. *Науковий вісник публічного та приватного права*. 2021. Випуск 6. Том 2. С. 170–174. URL: http://nvppp.in.ua.
67. Бойченко О. В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія.

Крим. юрид. ін-т ОДУВС. Сімферополь : Сімфероп. міська друк., 2009. 288 с.
68. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: http://www.crime-research.iatp.org.ua/library/strateg.htm.
69. Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права*. 2015. № 2. С. 77–78.
70. Борисова С. Є. Психологічні особливості осіб, які вчинили шахрайство, та їх облік під час розслідування злочинів. *Прикладна юридична психологія*. 2008. № 1. С. 108–115.
71. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* Київ: МНДЦ, 2009. № 19. С. 240– 247.
72. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» і «злочинність у сфері високих інформаційних технологій». *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2010. Вип. 23. С. 302–307.
73. Бутузов В. М. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2007. № 17. С. 316–325.
74. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КІТ, 2010. 408 с.
75. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук : 12.00.01. Київ, 2018. 203 с. URL: http://library.megu.edu.ua:8180/jspui/bitstream/123456789/1525/1/dysertatsiya_Buyadzhy.pdf
76. В Ірпені затримали групу мародерів з награбованим майном мешканців: офіційний сайт видання Zahid.net URL: https://zaxid.net/v_irpeni_zatrimali_grupu_maroderiv_z_nagrabovanim_maynom_meshkantsiv_n1540156
77. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис... канд. політичних наук: спец. 23.00.04. Київ, 2018. 210 с.

78. Вартилецька І. А., Плугатир В. С. Кримінальне право України: альбом схем. Заг. ред. В. Я. Горбачевського. Національна академія внутрішніх справ України. К.: Атіка, 2003. 207 с.
79. Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. канд. юрид. наук : 12.00.07. Дніпропетровськ, 2012. 203 с.
80. Вирок Красноармійського міськрайонного суду Донецької області від 16 листопада 2015 року (справа № 35/3606/15-к). URL: http://www.reyestr.court.gov.ua/Review/53461747.
81. Вирок Ленінського райсуда м. Кіровограда від 24 лютого 2015 року по справі № 405/1660/14-к. URL http://www.reyestr.court.gov.ua/Review/42833218.
82. Вирок Першотравневого районного суда м. Чернівців від 22.05.2017 року по справі № 725/85/17. URL: http://www.reyestr.court.gov.ua/Review/66614097.
83. Вирок Стрийського міськрайонного суда Львівської області від 21 січня 2016 року по справі № 456/4615/15-к. URL: http://www.reyestr.court.gov.ua/Review/55146476.
84. Відкриті дані Головного управління Національної поліції України. Офіційний сайт Головного управління Національної поліції України. URL: https://www.npu.gov.ua/diyalnist/vidkriti-dani.
85. Віктимологія : навч. посіб. За ред. В. В. Голіни і Б. М. Головкіна. Харків : Право, 2017. 308 с.
86. Волевоз А. Г. Протидія комп'ютерним злочинам: правові засади міжнародного співробітництва. К.: Юрлітінформ, 2002, 338 с.
87. Волошина Н. М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2010. № 2. С. 53–56.
88. Всесвітній огляд економічних злочинів. URL: https:/ /www.pwc.com/ua/uk/.
89. Всесвітня зустріч на найвищому рівні з питань інформаційного суспільства. Матеріали офіц. сайту URL: http://www.un.org/ua/ events/pastevents/wsis.shtml
90. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200–203.

91. Гаркуша Ю.О. Кримінологічна характеристика злочинів, пов'язаних з використанням соціальних мереж. *Порівняльне аналітичне право*. 2015. № 6. С. 255–258. URL: http://www.pap.in.ua/6_2015/78.pdf.
92. Голіна В. В., Головкін Б. М., Валуйська М. Ю., Лисодєд О. В. та ін. Кримінологія: Загальна та Особлива частини: підручник. За ред. В. В. Голіни і Б. М. Головкіна. Х.: Право, 2014. 512 с.
93. Головкін Б. М. Корислива насильницька злочинність в Україні: феномен, детермінація, запобігання: монографія. Харків : Право, 2011. 440 с.
94. Головкін Б. М. Як стають жертвами злочинів. *Проблеми законності : зб. наук. праць*. 2017. Вип. 136. С. 161–172.
95. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: https://www.gurt.org.ua/articles/34602/.
96. Голубєв В. О. «Кібертероризм» – міф чи реальність? URL: www.crime-research.org. (Computer Crime Researc h Center – Центр дослідження комп'ютерної злочинності).
97. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Гуманітарний ун-т «Запорізький ін-т державного та муніципального управління», Запоріжжя, 2003. 250 с.
98. Голубєв В. О. Комп'ютерні злочини в банківській діяльності. З. : Павел, 1997. 118 с.
99. Голубєв В. О. Кримінологічна характеристика злочинів у сфері використання комп'ютерних технологій. URL: https://www.crime-research.org/library/Gol_tem2.htm.
100. Голубєв В. О. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. 296 с.
101. Горбенко І., Потій О., Черних С., Прокофьєв М. Системний аналіз переходу від концепції національної інформаційної політики до доктрини інформаційної безпеки України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науковотехнічний збірник*. 2017. Вип. 5. С. 12–26.
102. Гордієнко Є. Г., Карачевчев О. В. Окремі аспекти запобігання злочинам у сфері комп'ютерних технологій. *Актуальні питання діяльності правоохоронних органів у сфері протидії*

кіберзлочинності. Матеріали Міжнародної науково-практичної конференції м. Харків, 12 листопада 2014 р., С. 23.
103. Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: право, економіка*. 2015. Вип. 12. С. 93–98.
104. Грицун О.О. Кримінальний аспект міжнародної інформаційної безпеки. *Право і суспільство*. 2015. № 6. Ч. 2. С.142–147.
105. Грищук В. К. Кодифікація кримінального законодавства: проблеми історії і методології України. Львів: Світ, 1992. 165 с.
106. Грінчак В. А., Земан І. В., Когутич І. І., Марін О. К. Міжнародне кримінальне право (співробітництво держав у протидії злочинності): підручник. Харків: Право, 2019. 440 с.
107. Гуренко-Вайцман М. М. Рецензія на монографію О.В. Бойченка «Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади)». *Форум права*. 2009. № 3. С. 738–740.
108. Гусарєв С. Д. Діяльний підхід у дослідженнях юридичної діяльності. *Науковий вісник НАВСУ*. 2004. № 4. С. 30–39.
109. Гусарєв С. Д. Юридична діяльність: методологічні та теоретичні аспекти: авто- реф. дис. на здобуття наук. ступеня д-ра юрид. наук : спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових вчень». Київ, 2007. 35 с.
110. Гуцалюк М. В. Вдосконалення чинного законодавства з питань протидії кіберзлочинності та забезпечення кібербезпеки. «*Інформація і право*». 2017. № 2(21). URL: https://ippi.org.ua/sites/default/files/14_3.pdf.
111. Данилішина К. О. Американський чинник в процесі інформаційної глобалізації : автореф. дис. ... канд. політ. наук : 23.00.04. Одеса, 2004. 18 с.
112. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Х.: Фоліо, 2002. 285 с.
113. Дашян М. С. Право інформаційних магістралей. М. : Норма, 2007. 288 с.
114. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті», прийнята 12 грудня 2003 р. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/995_c57#Text.

115. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. URL http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.
116. Діордіца І. В. Адміністративно-правове регулювання кібербезпеки України. Дисертація на здобуття наукового ступеня доктора юридичних наук за спец. 12.00.07. Запоріжжя, 2018. 416 с. URL: http://phd.znu.edu.ua/page/aref/07_2018/Diorditsa_aref.pdf.
117. Діордіца, І. В. Поняття і зміст кіберзагроз на сучасному етапі. *Підприємництво, господарство і право*. 2017. № 4. С. 99–107.
118. Дмитрук М. М. Питання термінології у визначенні системи злочинів в сфері ІТ (досвід інших держав). Матеріали Міжнародної науково-практичної онференції «*Кібербезпека в Україні: правові та організаційні питання*». матеріали всеукр. наук.-практ. конф., м. Одеса, 17 листопада 2017 р. Одеса : ОДУВС, 2017. С. 16–18. URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/98552c21-6a35-42c9-9bed-e147361e6cd0/content
119. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : від 28 січ. 2003 р. ; ратиф. Україною 21 серп. 2006 р. Офіційний сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/laws/show/994_687.
120. Дрьомін В. М. Злочинність як соціальна практика: інституціональна теорія криміналізації суспільства: монографія. О.: Юридична література, 2009. 616 с.
121. Дрьомін В. Н. Глобалізація інформаційних систем як фактор глобалізації злочинності. *Інформаційні технології та безпека: зб. наук. праць*. К., 2002. Вип. 1. С. 54–61.
122. Дубов Д. В. Політико-комунікативна безпека України у євроінтеграційному контексті : дис.... канд. політ. наук : 21.01.01. Київ, 2007, 197 с.
123. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України*. 2010. Вип. 3. С. 129–136.
124. Єдиний звіт про кримінальні правопорушення по державі за жовтень 2021 року. Статистична інформація Офісу

Генерального прокурора. URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=114140&libid=100820&c=edit&_c=fo#.
125. Єрема М., Борисенко А., Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. Офіційний сайт «LIGAЗакон». URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.
126. Жабинець О. Й. Захист інформації та інформаційна безпека страхових компаній. *Економічний часопис*. 2014. № 7–8(2). С. 32–35.
127. Жінки в IT: портрет, плани, мотивація. URL: https://dou.ua/lenta/articles/it-woman/.
128. Загуменний О. О. Кримінологічна характеристика осіб, які вчиняють кіберзлочини. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності*. Харків, 2014. С. 121–122.
129. Заморська Л. І. Системний підхід у дослідженнях правової реальності. *Вісник Південного регіонального центру Національної академії правових наук України*. 2016. № 7. С. 38–44.
130. Запорожець О. Ю. Політика Європейського Союзу в сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин*. 2009. Випуск 87 (Частина ІІ). С. 38
131. Заява коаліції «За вільний Інтернет» «Пакет законопроектів щодо протидії кіберзлочинності та посилення санкційного механізму від 1 вересня 2020 року містить загрози для цифрових прав». URL: https://dslua.org/publications/paket-zakonoproektiv-shchodo-protydii-kiberzlochynnosti-ta-posylennia-sanktsiynoho-mekhanizmu-vid-1-veresnia-2020-roku-mistyt-zahrozy-dlia-tsyfrovykh-prav-zaiava-koalitsii-za- vilnyy-internet/.
132. Звіт Національної поліції України про результати роботи у 2021 р. URL: https://www.kmu.gov.ua/storage/app/sites/1/17civik2018/zvit2021/Zvit_NPU_2021_.pdf.
133. Звіт про роботу прокурора: офіційний сайт Офісу Генерального прокурора України. URL: https://old.gp.gov.ua/ua/statinfo.html/
134. Звіт щодо України про чинне законодавство і проекти законів, що доповнюють різні питання, пов’язані з кіберзлочинністю та електронними доказами, та вносять зміни до них 2016/DGI/JP/3608 від 3 листопада 2016 року. 169 с. URL: https://rm.coe.int/16806f3743.

135. Зелінська Н. А. Злочинність у кіберпросторі: міжнародно-правовий дискурс. *Актуальні проблеми держави і права*. 2013. Випуск 67. С. 465–477.
136. Зелінська Н. А., Андрейченко С. С., Дрьоміна-Волок Н. В., Коваль Д. О. Теорія та практика міжнародного кримінального права: підручник. За ред. проф. Зелінської Н.А. Одеса: Фенікс, 2017. 582 с.
137. Зелінський А.Ф Кримінологія: курс лекцій. Харків: Прапор, 1996. 260 с.
138. Зміцнення Програми Організації Об'єднаних Націй у галузі запобігання злочинності та кримінального правосуддя, особливо її потенціалу у сфері технічного співробітництва A/RES/63/195 URL: http://daccess-ddsny.un.org/doc/UNDOC/GEN/ N08/482/51/PDF/N0848251.pdf.
139. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. Вип. 3. С. 172–177.
140. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. Вип. 3. С. 172–177.
141. Іленков А. Термінологія та її роль у представленні знань. *Вісник Нац. ун-ту «Львівська політехніка». Серія «Проблеми української термінології».* 2009. № 648. С. 24–29.
142. Ілюк К. Інформаційна війна – це не тільки фейки. *Детектор медіа*. 31.03.2022. URL: https://ms.detector.media/propaganda-ta-vplivi/post/29264/2022-03-31-informatsiyna-viyna-tse-ne-tilky-feyky/.
143. Калюжний Р. А. Теоретичні та практичні проблеми використання обчислювальної техніки в системі органів внутрішніх справ (організаційно-правовий аспект): автореф. дис. …д-ра юрид. наук: спец. 12.00.02 «Державне право та управління; адміністративне право; фінансове право». Київ, 1992. 47 с.
144. Калюжний Р.А., Новицька Н. Б. Становлення інформаційного суспільства. *Правова інформатика*. 2006. № 3 (11). С. 17–22.
145. Карчевский Н. В. Кіберзлочин чи злочин у сфері використання інформаційних технологій? // Кібербезпека в Україні: правові

та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса : ОДУВС, 2016. С. 10–15.
146. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів). Дисертація на здобуття наукового ступеня кандидата юридичних наук. Луганськ: РВВ ЛАВС, 2002. 175 с.
147. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. ЕО Дідоренка, 2012. 230 с.
148. Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon: офіційний сайт Державної служби спеціального звязку та захисту інформації в Україні. URL: https://cip.gov.ua/ua/news/kiberataka-na-derzhavni-organizaciyi-ukrayini-z-vikoristannyam-shkidlivoyi-programi-cobalt-strike-beacon.
149. Кібератака на Укртелеком 28 березня: деталі офіційний сайт Державної служби спеціального звязку та захисту інформації в Україні. URL: https://cip.gov.ua/ua/news/kiberataka-na-ukrtelekom-28-bereznya-detali
150. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь: Офіційний сайт національного інституту стратегічних досліджень. URL: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf
151. Кіберзлочинність та відмивання коштів: посібник. Департамент фінансових розслідувань. Державна служба фінансового моніторингу України. К., 2013. С. 51.
152. Кіберполіція вилучила сервери розробника M.E.DOC у рамках розслідування атаки вірусу PETYA. URL: https://zn.ua/ukr/UKRAINE/kiberpoliciya-viluchila-serveri-rozrobnika-m-e-doc-u-ramkah-rozsliduvannya-ataki-virusu-petya-247475_.html.
153. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? Офіційний сайт видання «Lexinform». URL: https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/.
154. Коваленко Є. В., Плетньов О. В. Передумови загроз у сфері інформаційної безпеки та перспективи їх подолання. *Актуальні*

проблеми управління інформаційною безпекою України : зб. тез наук. доповідей X Всеукраїнська наук.-практ. конф., Київ, 4 квітня 2019 року. Нац. акад. СБУ. Київ, 2019. С. 57–61.
155. Колб О. Г., Бендовський Н. Г. Про деякі напрями діяльності, що стосується національної безпеки України. Держава та регіони. Науково-виробничий журнал. Серія: Право. 2021. № 2 (72). С. 82–87. DOI https://doi.org/10.32840/1813-338X-2021.2.14.
156. Колб О. Г., Бендовський Н. Г. Сингулярність загроз інформаційній та національній безпеці України. *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті члена Правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової (м. Харків,16 квіт.2021 р.). МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2021. С. 313–314.
157. Колб О., Горбач Л. Про деякі проблемні аспекти діяльності із забезпечення національної безпеки окремих сил сектора безпеки та оборони України. *Юридичний вісник. НУ «Одеська юридична академія».* 2020. С. 33–38. DOI: https://doi.org/10.32837/yuv.v0i5.1999.
158. Колб О.Г., Гаврисюк Т. Про деякі кримінально-правові заходи запобігання посяганням на інформаційну безпеку України. *Вектори модернізації економіки України в контексті сталого розвитку*: матеріали Всеукр. наук.-практ. Інтернет-конф. (м. Луцьк, 20–21 травня 2021 р.). Луцьк: Волинський інститут ім. В. Липинського ПрАТ «ВНЗ «МАУП», 2021. С. 89–91.
159. Коломієць А. М. Теоретичні та методичні основи формування інформаційно культури майбутнього вчителя початкових класів : автореф. дис. д-ра пед. наук : 13.00.04. Київ, 2008. 46 с.
160. Комп'ютерна злочинність. Навчальний посібник. Київ: Атіка, 2002. 232 с.
161. Конвенція ООН проти транснаціональної організованої злочинності : прийн. резолюцією 55/25 Ген. Асамблеї від 15 листоп. 2000 р. ; ратиф. із застереженнями і заявами законом України від 4 лют. 2004 р. No1433-15 Офіційний сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/ laws/show/995_789.10.
162. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності: Резолюція 55/25

Генеральної Асамблеї від 15 листопада 2000 року. Офіційний сайт Верховної Ради України. URL: http://zakon5.rada.gov.ua/laws/show/995_789.
163. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності, ухвалена Резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000р. Офіційний сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/laws/show/995_789.
164. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу, ухвалену 29 травня 2000 р. Офіційний сайт Верховної Ради України. URL: /https://zakon.rada.gov.ua/laws/show/994_238#Text.
165. Конвенція про інформаційне та правове співробітництво, що стосується «Інформаційних громадських послуг»: ETS № 180 від 4 жовт. 2001 р. Офіційний сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/laws/show/994_559
166. Конвенція Ради Європи про кіберзлочинність : від 23 листоп. 2001р.; ратиф. Україною 7 верес. 2005 р. // Офіційний вісник України. 2007. № 65. Ст. 2535.
167. Конгреси ООН з попередження злочинності та кримінального правосуддя: збірник матеріалів: у 3-х книгах. Підзаг. ред. В. В. Голіни. Київ–Харків: Право, 2013. 342 с.
168. Конституція України: Закон від 28.06.1996 року № 254к/96-ВР. База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/254 %D0 %BA/96 %D0 %B 2 %D1 %80.
169. Конфлікти між державами та організаціями у 2013 році перейдуть у кіберпростір URL: http://dt.ua/TECHNOLOGIES/konflikti_mizh_derzhavami_ta_organizatsiyami_u_2013_rotsi_pereydut_u_kiberprostir.html.
170. Концепція Національної програми інформатизації, затверджена Законом України від 4 лютого 1998 року № 75/98-ВР. База даних «Законодавство України» / ВР України. https://zakon.rada.gov.ua/laws/show/75/98-вр#Text.
171. Користін О. Є., Бутузов В. М., Василевич В. В. та ін. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. Київ : Скіф, 2012. 728 с.
172. Кравцова М. А. Поняття кіберзлочинності і її ознаки. *Часопис Київського університету права.* 2015. № 2. С. 320–324.

173. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.08. Харк. нац. ун-т внутр. справ. Харків, 2016. 16 с.
174. Кравцова М. О. Мотивація кіберзлочинів: дані емпіричного дослідження. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності. Харків, 2014. С. 90
175. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с.
176. Кримінальне право України: Особлива частина: підручник. За заг. ред. д-ра юрид. наук, проф., засл. діяча науки і техніки України Є.Л. Стрельцова. Харків, 2009. 496 с.
177. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р.№ 2341-III / База даних «Законодавство України» / ВР України URL: http://zakon4.rada.gov.ua/laws/show/2341-14.
178. Кримінальний кодекс України : наук.-практ. комент. : у 2 т. За заг. ред.: В. Я. Тація [та ін.]. 5-те вид., допов. Х. : Право, 2013. Т. 1–2. 436 с.
179. Кримінальний кодекс України, введений в дію Законом Української РСР від 28.12.1960 р. // Відомості Верховної Ради України УРСР. Офіц. вид. 1961 № 2. Ст. 14.
180. Кримінологічна характеристика кіберзлочинності: сучасний стан та тенденції розвитку. Офіційний сайт видання «Інтернаука». URL: https://www.inter-nauka.com/uploads/public/15457583442358.pdf.
181. Кримінологія. Особлива частина. Навч. посібник. За ред. проф. І.М. Даньшина. Х.: Право, 1999. С.8–9.
182. Крутських А. В., Сафонова І. Л. Міжнародне співробітництво в галузі інформаційної безпеки. URL: www.ict.edu.uaft002472 intcoop.pdf.
183. Кузубова Т. О. Правові засади інституту тимчасового доступу до речей і документів у кримінальному провадженні : дис. ... канд. юрид. наук. Харків, 2019. 250 с.
184. Лефтеров Л. В. Кримінологічна характеристика осіб, підозрюваних у кіберзлочинах. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2018. № 35, том 2. С. 65–68. URL: http://vestnik-pravo.mgu.od.ua/archive/juspradenc35/part_2/18.pdf

185. Литвак О. М. Злочинність, її причини та профілактика. К. : Україна, 1997. 168 с.
186. Литвин О. П. Методологія юридичного дослідження: Навчальний посібник для магістрів. *Академія муніципального управління*. К.: Видавничо-поліграфічний центр АМУ, 2009. 221 с.
187. Ліпкан В. А. Національна безпека України: навчальний посібник. 2-ге вид. К. : КНТ, 2009. 576 с.
188. Ліпкан В. А., Залізняк В. А. Систематизація інформаційного законодавства України : монографія. За заг. ред. В. А. Ліпкана. Київ : О. С. Ліпкан, 2012. 304 с.
189. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ : КНТ, 2006. 280 с.
190. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.
191. Лісовий В. Комп'ютерні» злочини: питання кваліфікації. *Право України.* 2002. № 2. С. 86–88.
192. Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю. *Право і безпека : науковий журнал. Харк. нац. ун-т внутрішніх справ.* 2014. № 1 (52). С. 85–89.
193. Лой А. Філософсько-методологічна культура науковця в світлі сучасних змін. Наукові та освітянські методології та практики. К.: ЦГО НАН України, 2003. С. 32–38.
194. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис.... канд. юрид. наук : 12.00.01. Київ, 2007. 20 с.
195. Максименко Ю. Є. Теоретико-правові засали забезпечення інформаційної безпеки України : дис... канд. юрид. наук : 12.00.01. Київ, 2007. 188 с.
196. Малик Я. Й., Береза О. І. Забезпечення інформаційної безпеки України у контексті світового досвіду. *Ефективність державного управління*. 2012. Вип. 32. С. 20–27.
197. Малій М., Біленчук П. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *Юридичний вісник.* URL: https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/.

198. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2(57). С. 107–113.
199. Маркова М. В. Інформаційно-психологічна війна: медико-психологічні наслідки та стратегії протидії. *Проблеми безперервної медичної освіти та науки*. 2016. № 4. С. 6–10.
200. Машков А. Про можливість застосування синергетичних підходів до дослідження державно-правової дійсності: постановка питання. Наукові та освітянські методи та практики. Київ: ЦГО НАН України, 2003. С. 141–148.
201. Методики визначення належності бюджетних програм до сфери інформатизації: Наказ Держкомзв'язку та інформацтизації України від 06.06.2003 р. № 97. URL: http://zakon3.rada.gov.ua/laws/show/z0512-03.
202. Микитчук А.В. Заходи запобігання кіберзлочинності в Україні. Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку. Харків, 2019. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf.
203. Міжнародне кримінальне право (співробітництво держав у протидії злочинності): підручник / В. А. Грінчак, І. В. Земан, І. І. Когутич, О. К. Марін. Харків: Право, 2019. 440 с., с. 140
204. Міжнародне співробітництво у сфері інформаційної безпеки (довідкова інформація). URL: www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256e320029b1ef?OpenDocument.
205. Міжнародний центр протидії кіберзлочинності: офіційний вебсайт. URL: https://iccc.pro/.
206. Музика А. А., Азаров Д. С. Законодавство України про кримінальну відповідальність за комп'ютерні злочини: науково-практичний коментар і шляхи вдосконалення. К: Вид-во Паливода А. В., 2005. 267 с.
207. Нечай Л. О. Інформаційна безпека суб'єктів господарювання та фактори її розвитку. *Управління розвитком*. 2013. № 17. С. 145–148.
208. Нікулеско Д. Кібербезпека: вразливі моменти. Юридична газета, 14 травня 2019. URL: http://yur- gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html.
209. Новицька Н. Б. Електронний документообіг та електронний цифровий підпис як запорука успіху електронної комерції. *Правова інформатика.* 2006. № 4 (12). С. 76–80.

210. Новицька Н. Б. Окремі питання щодо формування правової інформатики як науки та навчальної дисципліни. *Правова інформатика*. 2004. № 4. С. 34–37.
211. Номоконов В. А., Тропіна Т. Л. Кіберзлочинність як нова кримінальна загроза. *Кримінологія: вчора, сьогодні, завтра*. 2012. № 1. С. 45–55.
212. Окінавська Хартія глобального інформаційного суспільства від 22 липня 2000 р. No 998–163. [Okinawa Charter on Global Information Society] // Дипломатичний вісник. 2000. № 8. С. 51–56.
213. Олійник О.В. Стан забезпечення інформаційної безпеки в Україні. Юридичний вісник. 2014. № 2 (31). С. 59–65.
214. Оліярчик Т. Інтернет-шахраї: обдирають як липку! Офіційний сайт видання «Львівська пошта», №118 (1587), 01.11.2014 р. URL: https://www.lvivpost.net/lvivnews/n/27275.
215. Онищенко О. С., Горовий В. М., Попик В. І. та ін. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія. НАН України, Національна бібліотекака України ім. В.І. Вернадського. К., 2014. 214 с.
216. Організація і сучасні методи захисту інформації. Під заг. ред. С. А Дієва. та А. Г. Шаваєва К, 1998. С. 52
217. Організація об’єднаних націй: Україна. URL: https://ukraine.un.org/ uk.
218. Основи інформаційної безпеки України : навч. посіб. Кол. авторів; за заг. ред. А. І. Марущака. К. : Наук.-вид. центр НА СБ України, 2013. 388 с.
219. Основні завдання Департаменту кіберполіції Національної поліції України. Офіційний сайт Національної поліції України. URL: https://www.cybercrime.gov.ua/contacts.
220. Офіційний сайт Державної служби статистики України. URL: http://www.ukrstat.gov.ua/.
221. Пивоваров В. В., Бабійчук В. С., Бевза Д. О. Кримінологічний аналіз явища кіберзлочинності. *Юридичний науковий електронний журнал*. 2021. № 12. С. 351–355. URL: http://www.lsej.org.ua/12_2021/89.pdf.
222. Пивоваров В. В., Терещенко К. В. Шахрайство її банківськими картками: окремі питання віктимологічної профілактики. *Карпатський приватний часопис.* 2015. С. 132–137

223. Пилипчук В. Г. Системні правові проблеми формування інформаційного суспільства: зб. наук. ст. та тез; наукове повідомлення за матеріалами міжнародної науково-практичної конференції «*Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі*», (Харків, 26 жовтня 2012 р.). Х. : НДІ державногобудівництва та місцевого самоврядування, 2012. 214 с.
224. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету: серія «Право».* 2017. Випуск 42. 2017. С. 16.
225. Політанський В. С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». 2017. Випуск 43, том 1. С. 34–35.
226. Попко В. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського національного університету: серія «Право».* 2021. Випуск 66. С. 4.
227. Почепцов Г. Г. Теория комунікації Київ: Ваклер, 2001. 656 с.
228. Почепцов Г. Метапропаганда як домінування пропаганди над ідеологією, а не навпаки. Хвиля. 17.09.2018. URL: https://hvylya.net/analytics/society/metapropaganda-kak-dominirovanie-propagandyi-nad-ideologiey-a- ne-naoborot.html.
229. Почепцов Р. Пропаганда vs інформаційні операції: подібності та відмінності. Детектор медіа, 02.06.2019. URL: https://ms.detector.media/mediaanalitika/post/22973/2019-06-02-kontr-ne-vsegda-plokho-osobenno-esly-jeto- kontrpropaganda/.
230. Пояснювальна записка до проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» від 31.08.2020 р. Офіційний сайт Верховної Ради України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=69770&pf35401=534066.
231. Правдюк С. А. Класифікація інформаційних правопорушень. *Порівняльно-аналітичне право*. URL: http:// www.pap.in.ua.
232. Правдюк С.А. Комп’ютерні правопорушення та інформаційні правопорушення: аспекти співвідношення. *Науковий вісник*

Національного університету біоресурсів і природокористування України. 2013. Вип. 182. Ч. 3. С. 216–223.
233. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.02.2022 № 2149-IX. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.
234. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 берез. 2022 № 2149-IX. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.
235. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам: Закон України від 15 березня 2022 року № 2137-IX. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.
236. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних. Указ Президента України від 24.09.2001 № 891/2001 // Урядовий кур'єр від 03.10.2001. № 179. URL: https://zakon.rada.gov.ua/laws/show/891/2001#Text.
237. Про деякі прояви кіберзлочинності у місцях позбавлення волі. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії. (м. Харків, 26 вересня 2019 р.). Харків. Право, 2019. С. 49-51.
238. Про електронні комунікації: Закон України 16 грудня 2020 року № 1089-IX. Офіційний сайт Верховної Ради України. URL: https://ips.ligazakon.net/document/view/T201089?bl=.
239. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/n0015525-16#Text.
240. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

241. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України: розпорядження Кабінету Міністрів України від 11 липня 2018 р. № 481-р. / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/96/2016.
242. Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень. Указ Президента України від 14.07.2000 № 891/2000. Урядовий кур'єр від 22.07.2000. URL: https://zakon.rada.gov.ua/ laws/show/891/2000#Text.
243. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні // Урядовий кур'єр від 08.08.2000. URL: https://zakon.rada.gov.ua/laws/show/928/ 2000#Text.
244. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. Офіційний сайт Верховної Ради України. URL: http://zakon4.rada.gov.ua/laws/show/2657-12.
245. Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України 16. 01. 1997 року 3/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/3/97-вр#Text.
246. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7 червня 2016 року № 242/2016 URL: https://www.president.gov.ua/documents/2422016-20141
247. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII // Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355.
248. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР. Офіційний сайт Верховної Ради України. URL: http://zakon0.rada.gov.ua/laws/show/74/98-вр.
249. Про осіб, які вчинили кримінальні правопорушення: офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/ posts/ pro-osib-yaki-vchinili-kriminalni-pravoporushennya-2.
250. Про основні засади забезпечення кібербезпеки України: Закон України 5 жовтня 2017 року № 2163-VIII. Офіційний сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/ laws/show/2163-19.

251. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII // Сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
252. Про підрозділ. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/contacts/
253. Про проблеми кримінально-процесуального права, пов'язані з інформаційними технологіями: Рекомендації Ради Європи № R (95) 13 від 11 вересня 1995 року. *Правова інформатика*. 2006. № 3 (11). С. 96–97.
254. Про ратифікацію Європейської конвенції про взаємну допомогу у кримінальних справах та Додаткового протоколу 1978 року до Конвенції № 1433-IV : Закон України від 04.02.04 р. URL: http://zakon0.rada.gov.ua/laws/show/44/98- %D 0 %B2 %D1 %80.
255. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.05 р. № 2824-IV (2824-15). URL: http://zakon2.rada.gov.ua/laws/show/2824-15.
256. Про рішення ради національної безпеки і оборони України від 15 жовтня 2021 року «Про стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2022 року No 685/2021 / Офіційний веб-портал Президента України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n33.
257. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»: Указ Президента України від 01.05.14 р. № 449/2014. URL: www.president.gov.ua/documents/ 4492014-17157.
258. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.17 р. № 47/2017. URL: www.president.gov.ua/documents/472017-21374
259. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13 жовтня 2015 р. // Сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/ laws/show/831-2015-п.

260. Про участь громадян в охороні громадського порядку і державного кордону: Закон України від 22.06.2000 № 1835-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1835-14.
261. Про участь громадян в охороні громадського порядку і державного кордону : Закон України від 22.06.2000 № 1835-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1835-14.
262. Програма інтеграції України до Європейського Союзу. Програма від 14.09.2000 URL: http://zakon4.rada.gov.ua/laws/show/n0001100-00.
263. Продан Т.В. Кримінологічна характеристика кіберзлочинності. *Юридичний науковий електронний журнал*. 2023. № 3. С. 415-417. URL:https://archer.chnu.edu.ua/bitstream/handle/123456789/6939/96.pdf?sequence=1&isAllowed=y.
264. Пропозиції щодо проекту правок до процесуального законодавства України, що стосується кіберзлочинності та електронних доказів (2016/DGI/JP/3608) від 28 травня 2017 року. 30 с. URL: https://drive.google.com/drive/folders/1pIM2wTFZjAN1CbwqXh9qN0cWSKzAULtX.
265. Пропозиції щодо проекту правок до процесуального законодавства України, що стосується кіберзлочинності та електронних доказів (2016/DGI/JP/3608) від 28 травня 2017 року. 30 с. URL: https://drive.google.com/drive/folders/1pIM2wTFZjAN1CbwqXh9qN0cWSKzAULtX.
266. Проскуріна О. О. Сучасна політична культура України в умовах глобалізації інформаційного суспільства : дис.. д–ра політ. наук : 23.00.03. Київ, 2009. 393 с.
267. Протидія когнітивній війні: інформованість і стійкість. НАТО Ревю. 20.05.2021. URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html.
268. Прохоренко Є. Феномен кіберкультури в інформаційно-технологічному відтворенні соціуму : дис. ... канд. соціол. наук. : 22.00.04. Харків, 2008. 215 с.
269. Пушкаренко, П. І. Кіберзлочинність як новітній феномен тіньової економіки. *Проблеми і перспективи розвитку банківської системи України* : зб. наук. Праць. 2006. Т. 17. С. 75–82.

270. Пфо О. М. Аналіз кіберзлочинності як комплексної проблеми. *Актуальні задачі та досягнення в галузі кібербезпеки*: Матеріали всеукраїнської науково-практичної конференції 23–25 листопада 2016 року, м. Кропивницький. URL: https://core.ac.uk/reader/84825470.
271. Пфо О.М. Основні поняття і класифікація кіберзлочинності. URL: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/http://195.230.140.114/jspui/bitstream/123456789/5119/1/AUConferenceCyberSecurity_November2016_p33.pdf.
272. Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання та розміщення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) : автореф. дис... канд. юрид. наук : 12.00.08. Х., 2002. 237 с.
273. Резолюція Генеральної Асамблеї A/RES/69/204 «Використання інформаційно-комунікаційних технологій для розвитку». URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N14/711/45/PDF/N1471145.pdf
274. Резолюція Генеральною Асамблеєю A/RES/65/230 «Дванадцятий Конгрес Організації Об'єднаних Націй щодо попередження злочинності та кримінального правосуддя» URL: https://documents-dds.
275. Результати першого в Україні дослідження наявності доступу населення до високошвидкісного інтернету / Департамент цифрової трансформації, інформаційних технологій та е-урядування. URL: https://egov.dp.gov.ua/ua/novini-ta-podiyi/mediateka/rezultati-pershogo-v-ukrayini-doslidzhennya-nayavnosti-dostupunaselennya-do-visokoshvidkisnogo-internetu.
276. Рижко В. Методологія та інноваційні процеси в науці. *Наукові і освітянські методології та практики.* К.: ЦГО НАН України, 2003. С. 20–27.
277. Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Дис на здобуття наукового ступеня кандидата юридичних наук за спец. 12.00.08. Університет державної фіскальної служби України, Ірпінь 2019. 208 с. https://www.nusta.edu.ua/wp-content/uploads/2016/11/Dis-Ричка.pdf.
278. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних

машин (комп'ютерів), систем та комп'ютерних мереж. Дис. канд. юрид. наук. К., 2003. 200 с.
279. Рубан В. Я. Інформаційна безпека України: сутність та проблеми. *Стратегічна панорама*. 1998. № 3–4. С. 170.
280. Руденко Д.О. Боротьба з кіберзлочинністю – пріоритетний напрям роботи правоохоронних органів країни. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності*. Харків, 2014. С. 35–36
281. Рущенко І. П., Зубар Н. В. Війна інформації. *Оборонний вісник*. 2017. № 6. URL: https://maidan.org.ua/2017/09/kohnityvnabezpeka-pohlyady-z-vashynhtonu-moskvy-kyjeva.
282. Савінова Н. А. Кримінально-правова політика забезпечення інформаційного суспільства в Україні: дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Львів: ЛьвДУВС, 2013. 510 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/788/1/Савінова %20Н.А. %20 %20дис.pdf
283. Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. 144 с.
284. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. Теоретичні та прикладні питання економіки: зб. наук. праць. Київ : Видавничо-поліграфічний центр «Київський університет», 2009. Вип. 19. С. 338–342.
285. Сащенко М. І. Проблемні аспекти запобігання кіберзлочинності в Україні. *Молодий вчений*. 2022. № 1 (101). С. 17–20. URL: https://molodyivchenyi.ua/index.php/journal/article/view/3115/3084.
286. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького нац. ун-ту*. *Економічні науки*. 2016. № 1. С. 155–161.
287. Семиколенов В. М. Мораль в інформаційному суспільстві : дис. .. канд. філос. наук : 09.00.04. Сімферополь, 2006. 212 с.
288. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. С. 192–194.

289. Сергєєва Д. Б., Старенький О. С. Використання результатів негласних слідчих (розшукових) дій для проведення тимчасового доступу до речей і документів. *Вісник кримінального судочинства*. 2015. № 4. С. 70–80. URL: http://nbuv.gov.ua/UJRN/vkc_2015_4_11.
290. Сєдая Ю. С. Кібервійна: основні теоретичні положення. *Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення*: матеріали Всеукр. наук.-практ. конф., м. Маріуполь, 9 чер. 2017 р. Маріуполь. ДонДУУ, 2017. С. 249–252.
291. Сироїд Т. Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності*: матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. С. 194–196.
292. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. Київ : КНТ, 2007. 160 с.
293. Скрипник А. В. До проблеми імплементації конвенції про кіберзлочинність у кримінальне процесуальне законодавство України. *Юридичний науковий електронний журнал*. 2020. № 6. С. 243–247. URL: http://lsej.org.ua/6_2020/26.pdf.
294. Скубіна Т. В. Адміністративно-правове забезпечення інформаційної безпеки в органах державної податкової служби України : дис. ... канд. юрид. наук : 12.00.01. Київ, 2010. 189 с.
295. Скулиш Є. Д. Теоретико-методологічні засади визначення об'єкта та предмета кіберзлочинів. *Правова інформатика*. 2014. № 2 (42). 2014. С. 48.
296. Скулиш Є.Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право*. 2010. № 1(10). С. 93–100.
297. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. 2015. № 3(15). URL: https://ippi.org.ua/sites/default/files/solodka.pdf.
298. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Наукові праці Нац. авіаційного ун-ту. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 2(59). С. 110–115. DOI: https://doi.org/10.18372/2307-9061.59.15603.

299. Стартував проєкт із протидії кібершахрайству у фінансовому секторі. Офіційний сайт Національного банку України. URL: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori.
300. Стаценко-Сургучова І. С. Організаційно-правові засади інформаційно-аналітичної роботи в органах державної податкової служби України : автореф. дис.... канд. юрид. наук : 12.00.07. Ірпінь, 2008. 21 с.
301. Степлюк К. В. Кримінологічна характеристика кіберзлочинності: сучасний стан та тенденції розвитку. *International Scientific Journal «Internauka».* URL: https://www.internauka.com/uploads/public/15457583442358.pdf.
302. Стережіться «виплат»: ПриватБанк попереджає про нову схему шахрайства. Офіційний сайт «УНІАН». URL: https://www.unian.ua/economics/finance/shahraystvo-z-bankivskimi-kartkami-privatbank-poperedzhaye-pro-novu-shemu-mahinaciy-novini-ukrajina-11895471.html.
303. Стратегія національної безпеки України : Указ Президента України від 14 вересня 2020 року №392/2020. Офіційний сайт представництва Президента України. URL: https://www.president.gov.ua/documents/3922020-35037
304. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право*. 2018. № 6(18). С. 154–163.
305. Тарасовський Ю. Як український бізнес працює під час війни. Головні факти з дослідження Gradus Research. Forbes. 23.03.2022. URL: https://forbes.ua/ news/v-ukraini-35-biznesu-prizupinili-diyalnist-cher-ez-viynu-1-ne-planuyut-vidnovlennya-opituvannya-gradus-23032022-4950.
306. Тарасюк К. В. Прокурорський нагляд при розслідуванні комп'ютерних злочинів. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2012. № 10. С. 178–181.
307. Телійчук В.Г. Способи вчинення злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та заходи протидії. *Держава та регіони.* 2014. Вип. № 2 (44). С. 31–37.

308. Тихомиров Д. Наукові методологічні підходи під час дослідження державної політики у сфері безпеки. *Підприємництво, господарство і право*. 2020. № 3. С. 230–234.
309. Тихомиров О. Д. Юридична компаративістика: філософські, теоретичні та методологічні проблеми. Київ : Знання, 2005. 334 с.
310. Тихомиров О. О. Інформаційні правопорушення: теоретико-правова концепція. *Інформаційна безпека людини, суспільства, держави*. 2015. № 1 (17). 2015. С. 41.
311. Ткачук В. В. Інформатизація освіти як чинник формування інноваційно-інформаційного суспільства в Україні (філософський аналіз) : дис. ... канд. філос. наук : 09.00.10. Київ, 2010. 178 с.
312. Торбяк М. М. Кіберзлочинність як суспільне явище. Матеріали науклвл-практичної конференції *«Національна юридична освіта й наука в європейському та євроатлантичному вимірах»*. К., 2019. URL: http://elar.naiau.kiev.ua/bitstream/123456789/16158/1/Національна %20юридична %20освіта %20й %20наука %20в %20європейському %20та %20євроатлантичному %20вимірах_p198-201.pdf.
313. Торяник В. М. Інформаційна безпека як складова національної безпеки держави. Роль ЗМІ в забезпечення інформаційного суверенітету України. *Право і суспільство*. 2016. № 2. С. 151–156. URL: http://www.pravoisuspilstvo.org.ua/archive/2016/2_2016/part_1/28.pdf.
314. Туляков В. О. Сучасний стан і перспективи розвитку науки кримінального права. *Основні напрями розвитку кримінального права та шляхи вдосконалення законодавства України про кримінальну відповідальність*: матеріали між нар. наук.-практ. конф., 11–12 жовтня 2012 р. Редкол. В. Я. Тацій (голов. ред.), В. І. Борисов (заст. голов. ред.) та ін. Х.: Право, 2012. С. 65–71.
315. Тунік А. В. Правові основи захисту персональних даних : дис. ... канд. юрид. наук : 12.00.07. Київ, 2012. 229 с.
316. Увага! Нова кібератака групи Armageddon на державні органи України офіційний сайт Державної служби спеціального звязку та захисту інформації в Україні. URL: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-grupi-armageddon-na-derzhavni-organi-ukrayini.

317. Угода про асоціацію України з Європейським Союзом від 27 червня 2014 р. URL: https://www.kmu.gov.ua/diyalnist/yevropejska-integraciya/ugodapro-asociacyu
318. Угода про боротьбу з кіберзлочинністю. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf?OpenElement.
319. Ухвала Вищого антикорупційного суду від 18 лютого 2020 року (справа № 991/1414/20). URL: http://www.reyestr.court.gov.ua/Review/87793041.
320. Ухвала Вищого антикорупційного суду від 2 березня 2020 року (справа № 991/1819/20). URL: http://www.reyestr.court.gov.ua/Review/88013481.
321. Ухвала Гайсинського районного суду Вінницької області від 21 листопада 2018 року (справа № 129/3194/16-к). URL: http://www.reyestr.court.gov.ua/Review/77991352.
322. Ухвала Новокаховського міського суду Херсонської області від 12 лютого 2020 року (справа № 661/685/20). URL: http://www.reyestr.court.gov.ua/Review/87542742.
323. Ухвала Печерського районного суду м. Києва від 10 лютого 2020 року (справа № 757/5768/20). URL: http://www.reyestr.court.gov.ua/Review/87631331.
324. Ухвала Святошинського районного суду м. Києва від 23 червня 2020 року (справа № 759/7376/20). URL: http://www.reyestr.court.gov.ua/Review/90128550.
325. Ухвала Святошинського районного суду м. Києва від 4 серпня 2020 року (справа No 759/12632/20-к). URL: http://www.reyestr.court.gov.ua/Review/90931393.
326. Ухвала Херсонського міського суду Херсонської області від 29 січня 2020 року (справа № 766/1427/20). URL: http://www.reyestr.court.gov.ua/Review/87220375.
327. Фоменко О. В. Кіберзлочинність: сучасний стан та особливості віктимологічної профілактики. *Юридичний науковий електронний журнал*. 2017. № 6. С. 328–330. URL: http://lsej.org.ua/6_2017/97.pdf.
328. Фурашев В. М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика*. 2012. № 2. С. 51–59.

329. Харитоненко І. О. Феномен кіберзлочинності в сучасній кримінологічній теорії. *Часопис Київського університету права*. 2020. № 4. С. 401–404.
330. Хахановський В. Г. Організація підготовки фахівців по боротьбі зі злочинністю у сфері високих технологій. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2001. № 3. С. 202.
331. Цимбалюк В. С. Причини латентності комп'ютерної злочинності: *Наукові записки. Спеціальний випуск*. Том 19. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/90d6e64c-1287-48b9-804d-a421361ad983/content.
332. Цимбалюк В. С. Латентність комп'ютерної злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2001. № 3. С. 178.
333. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження**.** *Прикарпатський юридичний вісник.* 2018. Випуск 3(24). С. 158 –162. URL: http://www.pjv.nuoua.od.ua/v3_2018/2018_3.pdf#page=158.
334. Шапочка С. В. Класифікація шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства). *Наука і правоохорона.* 2015. № 1. С. 159–165. URL: http://nbuv.gov.ua/UJRN/Nip_2015_1_26.
335. Шевердін М. М. За що можуть ув'язнити айтівця. *Економічна правда*. 2021. URL: https://www.epravda.com.ua.
336. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 1 (27). 312–320.
337. Шикун В., Булик Д. Фінансове шахрайство на підприємствах та методи його запобігання. *Економічний часопис Волинського національного університету імені Лесі Українки*. 2023. № 1. С. 70–79.
338. Широкова–Мурараш О. Г., Акчурін Ю. Р. Міжнародно-правові заходи щодо упередження злочинності у сфері інформаційної безпеки. *Науковий вісник Інституту міжнародних відносин НАУ. Серія: економіка, право, політологія, туризм.* 2010. Вип. 2. С. 78–82.

339. Шопін А. Ю. Інформаційна безпека як фактор забезпечення конкурентоспроможності підприємства. *Управління розвитком*. 2013. № 17. С. 155–157.
340. Юрасов А.В. Основи електронної комерції: учень. М. : Гаряча лінія-Телеком, 2008. 480 с.
341. Юринець Ю. Л., Сопілко І. М., Бєлкін Л. М., Бєлкін М. Л. Дослідження проблем інформаційної безпеки України на засадах міждисциплінарного підходу: соціологія, психологія, право. *Юридичний науковий електронний журнал. Електронне наукове фахове видання.* 2020. № 7. С. 300–307.
342. Юртаєва К.В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права*. 2009. № 2. С. 434–441. URL: http://www.nbuv.gov.ua/e-journals/FP/2009-2/09ykvvkt.pdf.
343. Ющук О. Інформаційна безпека користувачів мережі Інтернет. *Наукові записки Нац. ун-ту «Острозька академія». Сер.: Культура і соціальні комунікації.* 2009. Вип. 1. С. 224–231.
344. Як протидіяти кібершахрайству у фінансовому секторі. Офіційний сайт видання The page. URL: https://thepage.ua/ua/news/yak-protidiyati-kibershahrajstvu-u-finansovomu-sektori.
345. Якубівська Ю. Є. Світові тенденції розвитку кіберзлочинності. *Зовнішня торгівля: економіка, фінанси, право. Серія. Економічні науки.* 2014. № 5–6 (76–77). URL: http://zt.knute.edu.ua/files/2014/5-6(76-77)/uazt_2014_5-6_14.pdf
346. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ.* 2016. № 2. С. 244–252.
347. Яхно О. М. Україна в сучасному геополітичному просторі (політико-медійний аспект) : дис.... канд. політ. наук : 23.00.03. Київ, 2006. 170 с.
348. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС Украни (економіка, право),* 2014. № 2(65). С. 57.
349. Яцик Т. П. Розслідування інформаційного тероризму та кібертероризму (міжнародно-правовий аспект). *Міжнародний*

юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2017. Випуск 1 (5). С. 112.
350. Яцик Т. П., Кисла К. О., Пушкарьова Т. М. Кіберзлочинність в Україні: аналіз дієвості способів розслідування кіберзлочинів і напрями їх вдосконалення. *Юридичний науковий електронний журнал*. 2019. URL: http://www.lsej.org.ua/1_2019/51.pdf.
351. 2001 SCI/FBI Computer Crime and Security Survey. Computer Security Institute. 2001. №6. P.9.
352. 2020 Data Breach Investigations Report. Verizon. 2020. URL: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations- report.pdf.
353. A Brief History of Computer Crime: An Introduction for Students. M. E. Kabay, PhD, CISSP-ISSMP Program Director, MSIA School of Graduate Studies Norwich University. URL http://www.mekabay.com/overviews/history.pdf.
354. Abi Tyas Tunggal, Kaushik Sen. Cybersecu- rity Vs. Information Security. What's the Difference? 01.06.2022. UpGuard. URL: https://www.upguard.com/blog/cyber-securityinformationsecurity#:~:text=Cybersecurity
355. ASLU v.Reno, 929 F. Supp 824 (E.D.Pa.1996).
356. Assessment report Implementation of the preservation provisions of the Budapest Convention on Cybercrime, adopted by the T-CY at its 8 th Plenary (5–6 December 2012). 132 p. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0 9000016802e722e.
357. Barysevich A. Inside the Mind of Cybercriminals. URL: https://www.recordedfuture.com/cyber-criminal-profiling/
358. Bodunova O. To determining the scientific bases of determination of crime in the field of information technologies. *The scientific heritage (Budapest, Hungary)*. No 49 (2020). P.6. 48–51.
359. Bodunova O., Stefanchuk M., Polyvoda V., Kikalishvili M., Yeromenko-Kniazieva L. Digitalization of public services in countering criminal offenses. *Estudios Ekonomia Aplicada*. Volume 38–3 (1). ISSN 1133–3197 (Scopus).
360. Bodunova O., Yatsyk T., Luhina N. Participation of mass media in detection of crimes in martial law in Ukraine (on the example of Irpin, Kyiv region). *Ірпінський юридичний часопис* (спецвипуск). 2023. № 2 (11). С. 76–89.

361. Bodunova O., Omelchuk O., Shekhovtsova L., Lukasevych-Krutnyk I., Yanishevska K., Plutytska K. Criminal-legal and criminological research of illicit trafficking in narcotic drugs and their analogues with the use of computer technologies. *International Journal of Management (IJM).* Volume. Issue 6. June 2020, pp. 728–738. Article ID: IJM_11_06_060. Available online at http://www.iaeme.com/ijm/issues.asp?JType=IJM&VType=11&IType=6.
362. Bodunova O.M., Yatsyk T.P., Shkelebei V.A. Media interaction with law enforcement agencies as a factor in promoting crime prevention in the information sphere. *Fundamental and applied researches in practice of leading scientific schools.* Volume 38, Number 2, 2020. P. 15–20.
363. Brenner S.W. Toward a Criminal Law for Cyberspace A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J.1 (2004)
364. Computer Crimes Act http://www.clas.ufl.edu/docs/flcrimes/section2_1_1.html#SECTION00110000000000000000.
365. Cyber Intelligence Sharing and Protection Act. – Режим доступу : https://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act
366. Cyber's Most Wanted. URL: https://www.fbi.gov/wanted/cyber
367. Cybersecurity is a fascinating and highly scientific field spanning a range of disciplines and involving a wealth of organisations and actors, from both the public sector and the business world, within France and internationally. URL: http://www.ssi.gouv.fr/en/mission/word-from-director-general/
368. Document C-(2002)49: Security within tne North Atlantic Treaty Organization (NATO): [Online tool]. URL: www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf.
369. Electronic Frontier Foundation URL: www.eff.org/cyberspace-independence
370. Explanatory Report to the Convention on Cybercrime (Budapest, 23.XI.2001). 60 p. URL: https://rm.coe.int/16800cce5b.
371. Fasulo P. Cybersecurity vs Information Security: What's the difference? *Security Scorecard*. 2020. URL: https://securityscorecard.com/blog/information-security-versus-cybersecurity.

372. Framework for Improving Critical Infrastructure Cybersecurity 2016. URL: http://csrc.nist.gov/groups/SMA/forum/documents/ january2016_presentations/Cybersecurity-Framew ork-for-FCSM-Jan-2016.pdf
373. Fruhlinger J. What is information security? Definition, principles, and jobs. CSO United States. 17.01.2020. URL: https://www.csoonline.com/ article/3513899/what-is-information-security- definition-principles-and-jobs.html.
374. Information Security and Cyber Security: The Key Differences and Similarities. Simplilearn. 2021. URL: https://www.simplilearn.com/ information-security-vs-cyber-security-article.
375. Information Teenhology Security Evaluation Criteria: [Online tool]. – URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITS icherheitskriterien/itsec-en_pdf.pdf.
376. Irwin L. What's the difference between in- formation security and cyber security? IT Govern- ance. 2020. URL: https://www.itgovernance.eu/ blog/en/whats-the-difference-between-information- security-and-cyber-security.
377. It Security vs Cyber Security – What is the Difference? Logsign. 2020. URL: https://www.logsign.com/blog/it-security-vs-cyber-security-what-is-the-difference/.
378. Jānis Bērziņš. Russia's New Generation Warfare in Ukraine: *Implications for Latvian Defense Policy. Policy Paper*. April 2014. № 02. P. 5–13.
379. Jarrett, H. Marshall; Bailie, Michael W. (2010). Office of Legal Education Executive Office for United States Attorneys. Retrieved June 3, 2013. 213 p. URL: https://www.justice.gov/sites/default/files/ criminalccips/legacy/2015/01/14/ccmanual.pdf.
380. Liashuk O. M., Yatsyk T. P. Mass media as a factor in promoting the implementation of international wanted persons: Monograph. Actual problems of the humanities. Volum 1. Vienna 2015, «East West» Association for Advanced Studies and Higher Education GmbH. C. 29.
381. Loi 78–17 du 6 janvier 1978 modifiée URL: https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978- modifiee.
382. Loi favorisant la diffusion et la protection de la création sur Internet URL: http://www.senat.fr/dossier-legislatif/pjl07-405.html.

383. Marshall H.J. et al. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington, DC: U.S. Department of Justice. 2009. 299 p. URL: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.
384. National Security Inside a Russian disinformation campaign in Ukraine in 2014. Архів оригіналу за 25 грудня 2017. URL: https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html
385. NATO – Cyber defence. URL: //www.nato.int/cps/en/natohq/ topics_78170.htm
386. NATO Bucharest Summit Declaration, 3 April 2008: URL: http://www.nato.int/docu/pr/2008/p08-049e.html
387. NATO Lisbon Summit Declaration, 20 Nowember 2010: URL: http://www.nato.int/docu/pr/2010/ p10-049e.html.
388. NATO Warsaw Summit Communiqué, 9 July 2016: URL: http://www.nato.int/cps/en/natohq/ official texts 133169.htm.
389. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation: URL: http://www.nato.int/ lisbon2010/ strategic-concept-2010-eng.pdf.
390. Reimers K., Andersson D. Post-secondary education network security: the end user challenge and evolving threats. ICERI2017 Proceedings. 2017. Pp. 1787–1796. DOI: https://doi.org/ 10.21125/iceri.2017.0554.
391. Rohatynska Nina, Butkov Oleh, Butkova Olena, Burdonosova Maryna, Sukhorebra Tetiana. Use o information and communication technologies in democratic processes. *Cuestiones Politicas*. 2022. Vol. 40, Nº 75. C. 198–220.
392. Schatz D., Bashroush R., Wall J. Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. 2017. No 2. C. 54–74. DOI: https://doi.org/ 10.15394/jdfsl.2017.1476.
393. Stein A.R. Simposium: Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulator Precision. 98 Nw. U.L.Rev. 411 (2004).

394. The Global Risks Report 2019 (14th Edition). World Economic Forum. URL: http://www3.weforum.org/docs/WEF_ Global_Risks_Report_2019.pdf.
395. The USA Patriot Act: Preserving Life and Liberty. URL: //www.justice.gov/ /ll/highlights.htm.
396. Topchii, V., Zadereiko, S., Didkivska, G., Bodunova, O., Shayturo, O. Combating corruption: International standards and national practice. *Amazonia Investiga*, *11*(52), 278–287. https://doi.org/10.34069/AI/2022.52.04.30.
397. U.S. Code § 1029 – Fraud and Related Activity in Connection with Access devices. – Режим доступу : //www.law.cornell.edu/uscode/text/18/1029.
398. U.S. Code § 1030 – Fraud and related activity in connection with computers. – Режим доступу : //www.law.cornell.edu/uscode/ text/18/103.
399. U.S. Code Chapter 119 – Wire and electronic communications interception and interception of oral communications. URL: www.law.cornell.edu/uscode/text/ 18/part- I/chapter-119.
400. Vasyl Topchii, Svitlana Zadereiko, Galyna Didkivska, Olesia Bodunova, Dmytro Shevchenko. International anti-corruption standards. *Baltic Journal of Economic Studies*. Vol. 7 No. 5, 2021. DOI: https://doi.org/10.30525/2256-0742/2021-7-5-277-286.
401. What is Cyber Security? Definition and Best Practices. IT Governance. 2020. URL: https://www.itgovernance.co.uk/what-is-cybersecurity.
402. Who Are Cyber Criminals? Academic Programs & Resources. Information Security & Assurance by Norwich University Online. February 13th, 2017. URL: https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/articles/ who-are-cyber-criminals Profiling the Cybercriminal. URL: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/profiling-cybercriminal
403. Yatsyk T.P., Shkelebei V.A. Investigation of new forms of cybercrime (phishing and cybersquatting). *Національний вісник Ужгородського національного університету*. 2018. Випуск 53. Том 2. С. 122.
404. Yuzikova N., Khomiachenko S., Korniakova T., Chasova. T. Moral and psychological features of the motivational sphere of juveniles who commit crimes: risk assessment of determining

communication. *European Journal of Sustainable Development* 2021. Vol.10,1, p.123–135. Doi: 10.14207/ejsd.2021.v10n1p123 European Journal of Sustainable Development https://ecsdev.org/ojs/index.php/ejsd/issue/view/42.

Для нотаток

Для нотаток

Наукове видання

БОДУНОВА ОЛЕСЯ МИКОЛАЇВНА

ТЕОРЕТИКО-ПРИКЛАДНІ ОСНОВИ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Монографія

Друкується в авторській редакції
Технічний редактор *І. С. Талімончук*

Формат 60х84 1/16. Обсяг 20,00 ум. друк. арк., 19,70 обл.-вид. арк.
Наклад 300 пр. Зам. 173. Виготовлювач – Вежа-Друк
(м. Луцьк, вул. Шопена, 12, тел. +38 066-936-25-49)
Свідоцтво Держ. комітету телебачення та радіомовлення України
ДК № 4607 від 30.08.2013 р.