

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ,
ПСИХОЛОГІЇ ТА БЕЗПЕКИ

Кафедра менеджменту та економічної безпеки

**ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ
КІБЕРЗЛОЧИННОСТІ**

кваліфікаційна робота
здобувача вищої освіти
2 курсу денної форми навчання
ЯСІНЯ ВАСИЛЯ ІВАНОВИЧА

Науковий керівник
доктор економічних наук, професор
МЕЛЬНИК Степан Іванович

Рецензент
кандидат економічних наук, доцент
НАКОНЕЧНА Наталія Володимирівна

Кваліфікаційна робота допущена до захисту
«9» грудня 2024 р., протокол № 1
завідувач кафедри менеджменту
та економічної безпеки

_____ **КОПИТКО М. І.**

Львів
2024

АНОТАЦІЯ

ЯСІНЬ В.І. – Протидія легалізації доходів, отриманих у сфері кіберзлочинності. – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 072 «Фінанси, банківська справа, страхування та фондовий ринок». – Львівський державний університет внутрішніх справ МВС України, Львів, 2024.

Кваліфікаційна робота присвячена обґрунтуванню теоретико-прикладних аспектів дослідження проблем протидії легалізації доходів, отриманих у сфері кіберзлочинності. Розглянуто сутність і причини легалізаційних процесів та їх наслідки для національної економіки, розкрито поняття кіберзлочинності, її види та способи протидії. Проведено аналітичні дослідження сучасного стану кіберзлочинності в Україні та оцінювання обсягів легалізації доходів, отриманих у сфері кіберзлочинності. Запропоновано основні заходи щодо удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності та узагальнено міжнародний досвід її удосконалення.

Ключові слова: легалізаційні процеси, кіберзлочинність, кіберпростір, кіберзлочини, протидія легалізації доходів, кібербезпека.

ANNOTATION

YASIN V.I. – Combating the legalization of proceeds received in the field of cybercrime. – Manuscript.

Qualification work for the master's degree in the specialty 072 "Finance, banking, insurance and stock market". – Lviv State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Lviv, 2024.

The qualification work is devoted to the substantiation of the theoretical and applied aspects of researching the problems of combating the legalization of income obtained in the field of cybercrime. The essence, causes of legalization processes and their consequences for the national economy are considered, the concept of cybercrime, its types and countermeasures are revealed. Analytical studies of the current state of cybercrime in Ukraine and assessment of the amount of legalization of income received in the field of cybercrime were conducted. The main measures to improve the system of combating the legalization of income obtained in the field of cybercrime are proposed and the international experience of its improvement is summarized.

Key words: legalization processes, cybercrime, cyberspace, cybercrimes, combating money laundering, cyber security.

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1. ТЕОРЕТИЧІ ОСНОВИ ДОСЛІДЖЕННЯ ПРОБЛЕМ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ.....	7
1.1. Сутність, причини легалізаційних процесів та їх наслідки для національної економіки.....	7
1.2. Поняття кіберзлочинності, її види та способи протидії.....	14
Висновки до розділу 1.....	22
РОЗДІЛ 2. АНАЛІЗ СТАНУ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ ТА ПРОБЛЕМ ЇЇ ПРОТИДІЇ В КОНТЕКСТІ ЗАПОБІГАННЯ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ ЗЛОЧИННИМ ШЛЯХОМ.....	23
2.1. Сучасний стан кіберзлочинності в Україні.....	23
2.2. Оцінювання обсягів легалізації доходів, отриманих у сфері кіберзлочинності.....	32
Висновки до розділу 2.....	38
РОЗДІЛ 3. УДОСКОНАЛЕННЯ ЗАХОДІВ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ.....	40
3.1. Стратегічні пріоритети протидії кіберзлочинності.....	40
3.2. Міжнародний досвід удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності.....	47
Висновки до розділу 3.....	54
ВИСНОВКИ.....	56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	59

ВСТУП

Актуальність теми дослідження. Посилення процесів глобалізації, сучасні виклики геополітизації та зміни світового порядку, що супроводжуються наявністю вагомих викликів і небезпек, обумовлюють необхідність інтенсифікації розвитку цифрових інформаційних технологій та їх залучення в систему функціонування фінансово-економічних відносин. Поряд із позитивними аспектами цифровізації держави і суспільства в умовах сьогодення загострюються проблеми використання інформаційних технологій та кіберпростору у злочинних цілях та спостерігається стрімкий розвиток кіберзлочинності, яка перетворилася у загрозливе транснаціональне явище і становить істотну загрозу інтересам України. Крім того, активізація злочинності у кіберпросторі зумовлює зростання обсягів неправомірно одержаних капіталів, які потребують узаконення та залучення в офіційний сектор національної економіки, що призводить до розвитку такого деструктивного явища як легалізація (відмивання) доходів, одержаних злочинним шляхом. Очевидно, що окреслені тенденції засвідчують актуальність тематики дослідження, яка пов'язана із виявленням проблемних питань протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Теоретико-прикладні аспекти дослідження системи протидії легалізації доходів, отриманих у сфері кіберзлочинності, знаходять своє відображення у наукових розробках як вітчизняних, так і зарубіжних вчених. Ґрунтовні напрацювання із зазначеної проблематики належать Л. Аркуші, О. Беху, І. Білоус, В. Гончаруку, Л. Грабовському, І. Завидняк, Н. Лугіній, Я. Неділько, Н. Никончук, М. Уткіній, Д. Чебуркіній, С. Фролову та ін., які розкривають основні засади зазначеної проблематики. Крім напрацювань зазначених науковців, в процесі написання кваліфікаційної роботи використано закони України, міжнародні конвенції, аналітичні й звітні дані Національної поліції України, Державної служби фінансового моніторингу України, міжнародних

організацій, а також інформаційні ресурси мережі Інтернет. Однак, не заперечуючи вагомих здобутків щодо дослідження протидії легалізації доходів, отриманих у сфері кіберзлочинності, невирішеною залишається проблема зниження темпів поширеності кіберзлочинності та методів боротьби із даним небезпечним соціально-економічним явищем.

Мета і завдання дослідження. Мета кваліфікаційної роботи полягає в обґрунтуванні теоретичних засад та практичних аспектів забезпечення ефективної протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Для досягнення поставленої мети дослідження необхідним виявляється вирішення наступних завдань:

- визначити сутність і причини легалізаційних процесів та їх наслідки для національної економіки;
- здійснити дослідження поняття кіберзлочинності, визначити її види та способи протидії;
- проаналізувати сучасний стан кіберзлочинності в Україні;
- оцінити обсяги легалізації доходів, отриманих у сфері кіберзлочинності;
- окреслити стратегічні пріоритети протидії кіберзлочинності;
- систематизувати міжнародний досвід удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Об'єктом дослідження є система протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Предметом дослідження є теоретичні засади та прикладні аспекти дослідження системи протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Методи дослідження. У кваліфікаційній роботі використано загальнонаукові методи та спеціальні прийоми наукового дослідження. Зокрема, метод системного аналізу, компаративний аналіз, спостереження та групування застосовано для визначення сутності досліджуваних категорій кіберзлочинності та легалізаційних процесів. Метод статистичного аналізу,

порівняння, аналітичний метод та функціонально-системний підхід застосовані в процесі проведення емпіричних досліджень, пов'язаних із аналізом сучасного стану кіберзлочинності в Україні та оцінками обсягів легалізації доходів, отриманих у сфері кіберзлочинності. Метод абстрагування, систематизації та узагальнення використані для формування результатів дослідження та висновків.

Наукова новизна одержаних результатів:

– удосконалено основні стратегічні напрямки протидії кіберзлочинності шляхом надання пропозиції доповнення чинного законодавства у сфері протидії даному деструктивному явищу. Обґрунтовано необхідність розроблення та прийняття Закону України «Про державно-приватне партнерство у сфері кібербезпеки», а також розроблення та реалізації Загальнодержавної програми кіберграмотності населення.

Основний зміст роботи. Кваліфікаційна робота складається із трьох розділів. У першому розділі визначено сутність і причини легалізаційних процесів та їх наслідки для національної економіки, а також здійснено дослідження поняття кіберзлочинності, визначено її види та способи протидії. Другий розділ кваліфікаційної роботи присвячено аналізу сучасного стану кіберзлочинності в Україні та проведенню оцінок обсягів легалізації доходів, отриманих у сфері кіберзлочинності. У третьому розділі роботи окреслено стратегічні пріоритети протидії кіберзлочинності та систематизовано міжнародний досвід удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Структура роботи. Кваліфікаційна робота складається із анотації українською та англійською мовами, вступу, трьох розділів, висновків та списку використаних джерел (49 найменувань на 6 сторінках). Загальний обсяг роботи становить 64 сторінки, з яких основний текст – 52 сторінки, в тому числі 15 рисунків.

РОЗДІЛ 1

ТЕОРЕТИЧІ ОСНОВИ ДОСЛІДЖЕННЯ ПРОБЛЕМ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

1.1. Сутність, причини легалізаційних процесів та їх наслідки для національної економіки

Посилення процесів трансформації світового співтовариства у відкриту систему соціально-економічних, суспільно-політичних та інформаційно-технологічних відносин обумовлює виникнення вагомих глобальних проблем, що чинять негативний вплив на національні економіки та активізують розвиток дестабілізуючих чинників, процесів і явищ фінансово-економічного та соціального характеру, одним із яких виявляється легалізація (відмивання) доходів, одержаних злочинним шляхом. В умовах глобалізації та обрання курсу на євроінтеграцію дестабілізуючі чинники розвитку економіки країни особливо загострили свою негативну дію та поширюють свій вплив на суспільство і державу. Активізація протиправної економічної діяльності в тіньовому секторі економіки призводить до значного накопичення нелегально одержаних капіталів, які потребують узаконення та залучення в офіційний обіг, що, своєю чергою, стимулює розвиток легалізаційних процесів.

Існуючі наукові погляди на визначення сутності легалізаційних процесів, окреслення причин їх виникнення та оцінювання наслідків для національної економіки зосереджені на трактуванні легалізації (відмивання) доходів, одержаних злочинним шляхом, як процесу набуття, використання, володіння та розпорядження грошовими коштами, майном та іншими активами, які одержані у протиправний спосіб внаслідок здійснення неправомірних фінансових операцій та правочинів із майном, що пов'язані із

їх переміщенням, перетворенням, приховуванням та маскуванню джерел їх походження, використання й реального місця знаходження.

О. Бех [1, с. 214] наголошує на тому факті, що існуючі світогосподарські порядки сприяють розвитку легалізаційних процесів, оскільки розширюють соціально-економічні зв'язки, стимулюють розвиток міжнародних електронних банківських мереж та ускладнюють контроль за грошовими потоками на міжнародному рівні. Однак, Л. Аркуша [2, с. 141] доводить, що масштабність поширення легалізаційних процесів обумовлена важкістю та проблематичністю виявлення фактів вчинення злочинів, пов'язаних із легалізацією (відмиванням) доходів, одержаних злочинним шляхом, адже, даний вид злочинних діянь передбачає складність у виявленні, фіксуванні та встановленні причин їх вчинення. Більше того, виявлення фактів легалізації грошових коштів, майна та інших активів потребує своєчасного встановлення інформації, яка відображається у низці важливих документів фінансово-господарського характеру, які, як правило, перебувають у закритому доступі та становлять комерційну таємницю. Очевидно, що, як зазначає В. Гончарук [3, с. 129], легалізація злочинно одержаних коштів і майна виявляється суспільно небезпечним діянням та проявляється через вчинення посягань на громадські інтереси, шкоди від яких зазнає як держава, так і суспільство.

Н. Лугіна та М. Омелян [4, с. 159–160] легалізацію (відмивання) грошових коштів, майна та активів, що набуті у протиправний спосіб, трактують як процес переформування незаконно одержаної грошової маси в законні засоби, при якому замасковується їх нелегальне походження, існування та використання. Водночас, науковці виокремлюють найбільш вагомі причини легалізаційних процесів (рис. 1.1), а саме:

- 1) тісні неформальні взаємозв'язки всередині підприємницьких ділових груп та політичних структур;
- 2) лобіювання інтересів впливових осіб у державних структурах;
- 3) прагнення до самозбагачення посадових та службових осіб;

- 4) економічне шпигунство;
- 5) шахрайство;
- 6) корупція
- 7) інтенсифікація кіберзлочинності.

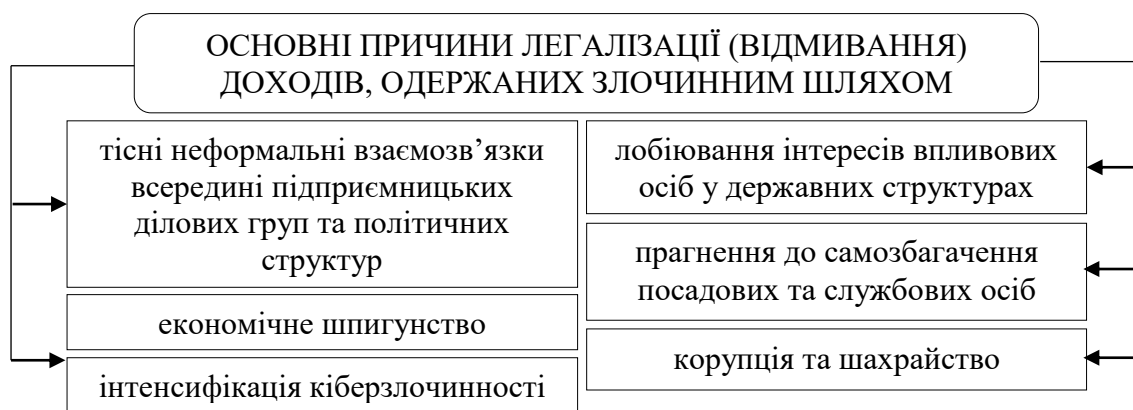


Рис. 1.1. Перелік причин виникнення легалізаційних процесів

Джерело: сформовано автором за даними: [4, с. 159–160]

Спільною ознакою причин виникнення легалізаційних процесів варто назвати прагнення до отримання неправомірної вигоди у різних її проявах та збагачення за рахунок тіньових капіталів.

Водночас, слушним є зауваження Н. Лугіної та М. Омелян [4, с. 161] щодо трактування легалізації (відмивання) доходів, одержаних злочинним шляхом, як небезпечного та вагомого злочину, який має певні ознаки, зокрема:

- 1) вчинення протиправних діянь, що містять ознаки легалізації, відбувається шляхом свідомого порушення усталених економічних відносин та створення нових на незаконних засадах;
- 2) предметом злочинних посягань є грошові кошти, майно та інші активи;
- 3) неформальні економічні відносини несуть збитки суб'єктам господарювання та загрожують стратегічним інтересам держави;
- 4) посилення нестабільності фінансової системи країни;

5) загострення суспільної небезпеки, що проявляється у порушенні й обмеженні конституційних принципів у площині забезпечення єдності економічного простору, вільного переміщення фінансових ресурсів та свободи економічної діяльності;

6) інтенсифікація розвитку організованої економічної злочинності;

7) зростання кількості фінансових центрів, за допомогою яких в короткі терміни проводяться фінансові операції, спрямовані на легалізацію тіньових капіталів.

В даному контексті, зважаючи на особливості легалізаційних процесів, Д. Чебукіна [5, с. 187] пропонує розглядати суб'єктивну та об'єктивну сторону даного дестабілізуючого для економіки і суспільства явища. Зокрема, з точки зору автора, суб'єктивна сторона легалізації (відмивання) грошових коштів, майна та інших тіньових капіталів, здобутих у неправомірний спосіб, проявляється в існуванні прямого умислу на вчинення такого злочинного діяння. Тобто, злочинець усвідомлює кримінальне походження доходів, які прагне легалізувати, та чітко розуміє з якою метою вчинятиметься злочинне діяння. Натомість, об'єктивна сторона легалізації характеризується різносторонністю альтернативних дій, зокрема, здійсненням фінансових операцій чи правочину, що у своєму складі мають суспільно небезпечні діяння (предикатних легалізації злочинів); вчинення умисних дій задля приховування чи маскуванню тіньових капіталів; володіння та використання протиправно одержаних грошових коштів, майна та інших активів.

М. Бліхар, Н. Ортинська, О. Дуфенюк, М. Вінічук та О. Матвієнко [6] посилення процесів легалізації в країні пояснюють наявністю зростаючих тенденцій щодо тінізації економічних відносин на міжнародному рівні та створенням сприятливого середовища для узаконення нелегально одержаних капіталів. В даному контексті, науковцями акцентується увага на існуванні офшорних зон, які активно використовуються для легалізації (відмивання) злочинних капіталів за рахунок вагомих преференцій на їх територіях щодо

фіскального та валютно-фінансового режиму, захисту банківської таємниці та лояльності інституційного середовища.

На існуванні зручних та легально створених структур, які беруть участь у відмиванні й узаконенні грошових коштів, майна та активів, здобутих в тіньовому секторі економіки, наголошує І. Завидняк [7, с. 314–315], який виявив, що легалізація є транснаціональним явищем, а її процеси здійснюються із використанням міжнародної фінансово-економічної системи, яка дозволяє безперешкодно конвертувати злочинні активи та переводити їх за межі країни походження за допомогою спеціально створених структур.

Зважаючи на зазначене, можна стверджувати, що легалізація (відмивання) протиправно одержаних тіньових капіталів та майна виявляється типовим конвенційним злочином. В даному контексті, С. Фролов [8, с. 130] зауважив, що криміналізація легалізаційних процесів відбувається паралельно із набуттям державою приналежності до коаліції учасників міжнародно-правових актів у сфері антилегалізаційної боротьби.

На вагомості формування міжнародної системи протидії легалізації (відмиванню) доходів, походження яких є злочинним, наголошує М. Уткіна [9], яка стверджує, що лише консолідація зусиль міжнародної спільноти спроможна знизити темпи легалізації. Крім того, науковиця доводить обґрунтованість та доцільність розроблення, запровадження та імплементації міжнародних стандартів у сфері протидії легалізації (відмиванню) коштів, отриманих у неправомірний спосіб.

Більше того, М. Бліхар, М. Вінічук, І. Комарницька, О. Заяць та М. Кащук [10] доводять, що легалізаційні процеси в умовах нестабільності спричиняють гостру нестачу фінансових ресурсів та активізують розвиток економічної злочинності. При цьому, автори наголошують на виокремленні такого виду злочинності як кіберзлочинність, масштаби якої постійно зростають, а кіберпростір дедалі частіше використовується для здійснення фінансових операцій, пов'язаних із відмиванням нелегальних капіталів.

Стає очевидним, що легалізаційні процеси становлять значну загрозу інтересам держави, а їх наслідки є катастрофічними для економіки й суспільства. Варто зазначити, що І. Білоус [11, с. 87], а також М. Бліхар, Л. Савченко, І. Комарницька та М. Вінічук [12] виокремили найбільш небезпечні наслідки інтенсифікації розвитку легалізаційних процесів, до яких відносять наслідки як для економіки, так і для суспільства. Уніфікацію основних наслідків легалізації (відмивання) злочинно одержаних тіньових капіталів здійснимо на рис. 1.2.



Рис. 1.2. Основні наслідки легалізаційних процесів для економіки країни

Джерело: сформовано автором за даними: [11, с. 87; 12]

При цьому, зазначимо, що наслідки легалізації злочинно одержаних грошових коштів, активів та майна є вагомими та небезпечними, а в умовах запровадження спеціального правового режиму воєнного стану в державі посилюються чинниками невизначеності та нестабільності. Зокрема, необхідно сказати, що легалізаційні процеси істотно дестабілізують темпи соціально-економічного зростання та призводять до зростання соціальної нестабільності та макроекономічної кризи. Більше того, як стверджує Л. Грабовський [13, с. 202], процеси легалізації (відмивання) протиправно отриманих активів, грошових коштів та майна загрожують різкій диференціації суспільства за рівнем доходів та стимулюють зростання незначної частки багатого населення і його збагачення за рахунок ведення економічної діяльності в тіньовому секторі. Очевидно, що узаконені внаслідок легалізації активи можуть бути використані для продовження злочинної діяльності, або ж під виглядом інвестиційних ресурсів залучаються в офіційний сектор економіки в перспективні види економічної діяльності.

З іншої сторони, легалізаційні процеси обумовлюють значні втрати держави у фіскальній сфері, адже, тіньові капітали не оподатковуються та не залучаються до фінансової системи держави. Не менш вагомим є негативний вплив легалізаційних процесів на державний сектор, де дедалі частіше прослідковуються прояви корупції, підкупу державних службовців та посадових осіб.

Таким чином, проведені дослідження теоретичних аспектів легалізаційних процесів дозволили з'ясувати сутність легалізації (відмивання) доходів, одержаних злочинним шляхом, під якою розуміється вчинення діянь, пов'язаних із приховуванням джерел походження, місця знаходження та використання грошових коштів, майна та інших нелегальних активів з метою збагачення та одержання неправомірної вигоди. Встановлено, що причинами поширення легалізаційних процесів є значні накопичення тіньових капіталів, які потребують узаконення та залучення в офіційний сектор економіки. Доведено негативний вплив легалізаційних

процесів на національну економіку країни та на стан функціонування суспільства, який проявляється у зростанні соціальної нестабільності та соціальної напруги, а також у посиленні макроекономічної кризи, фінансової нестабільності та невизначеності. В процесі дослідження виявлено, що в умовах сучасності активізувалися схеми легалізації (відмивання) грошових коштів, які широко використовують комп'ютерні системи та інформаційні технології, а кіберпростір поступово трансформується у майданчик для вчинення злочинних діянь, що, своєю чергою актуалізує необхідність дослідження основних тенденцій кіберзлочинності.

1.2. Поняття кіберзлочинності, її види та способи протидії

В сучасних умовах функціонування держави і суспільства домінуючу роль відіграють інформаційні технології, застосування яких передбачає широке використання комп'ютерної техніки, мобільних засобів комунікації, мереж зв'язку та інших технічних засобів. Інформаційні технології виявляються ефективним інструментом нівелювання кордонів національних економік та функціонування єдиного глобального віртуального середовища – інформаційного простору. Очевидно, що поряд із позитивними аспектами розвитку кіберпростору та активізацією використання інформаційних технологій в фінансово-економічних процесах, загострилися проблеми їх участі як інструменту вчинення злочинів та ведення протиправної діяльності. Більше того, інформаційні технології на сучасному етапі широко використовуються з метою легалізації (відмивання) доходів, які отримані у протиправний незаконний спосіб. Одержання доступу злочинцями до інформаційно-комунікаційних систем та вчинення ними дій, що пов'язані із стороннім втручанням у бази даних, в автоматизовані системи управління та в систему банківських рахунків, вчинення фінансового шахрайства та

крадіжки даних платіжних карт, створюють вагомі загрози й кваліфікуються як кіберзлочини.

Дослідження існуючих науково-прикладних розробок доводять, що кіберзлочинність набула значних масштабів на світовому рівні та привертає увагу міжнародної спільноти. І. Діордіца [14] стверджує, що кіберзлочинність є актуальною та небезпечною проблемою сучасності, вагомість якої постійно зростає, а рівень спричиненої шкоди набуває катастрофічного значення як для держави, так і для суспільства. При цьому, науковець наголошує, що в національних офіційних нормативно-правових документах визначення категорії «кіберзлочинність» є достатньо обмеженим та не чітким, а її сутність розкривається крізь призму розуміння кіберзлочинності як одного із видів злочинної діяльності у сфері інформаційно-телекомунікаційних та комп'ютерних технологій, незаконного обігу радіоелектронних та спеціальних засобів зв'язку, а також щодо поширення неліцензійного програмного забезпечення. Дослідивши наукові праці з обраної проблематики І. Діордіца сформував декілька підходів до трактування сутності кіберзлочинності, які систематизуємо на рис. 1.3.

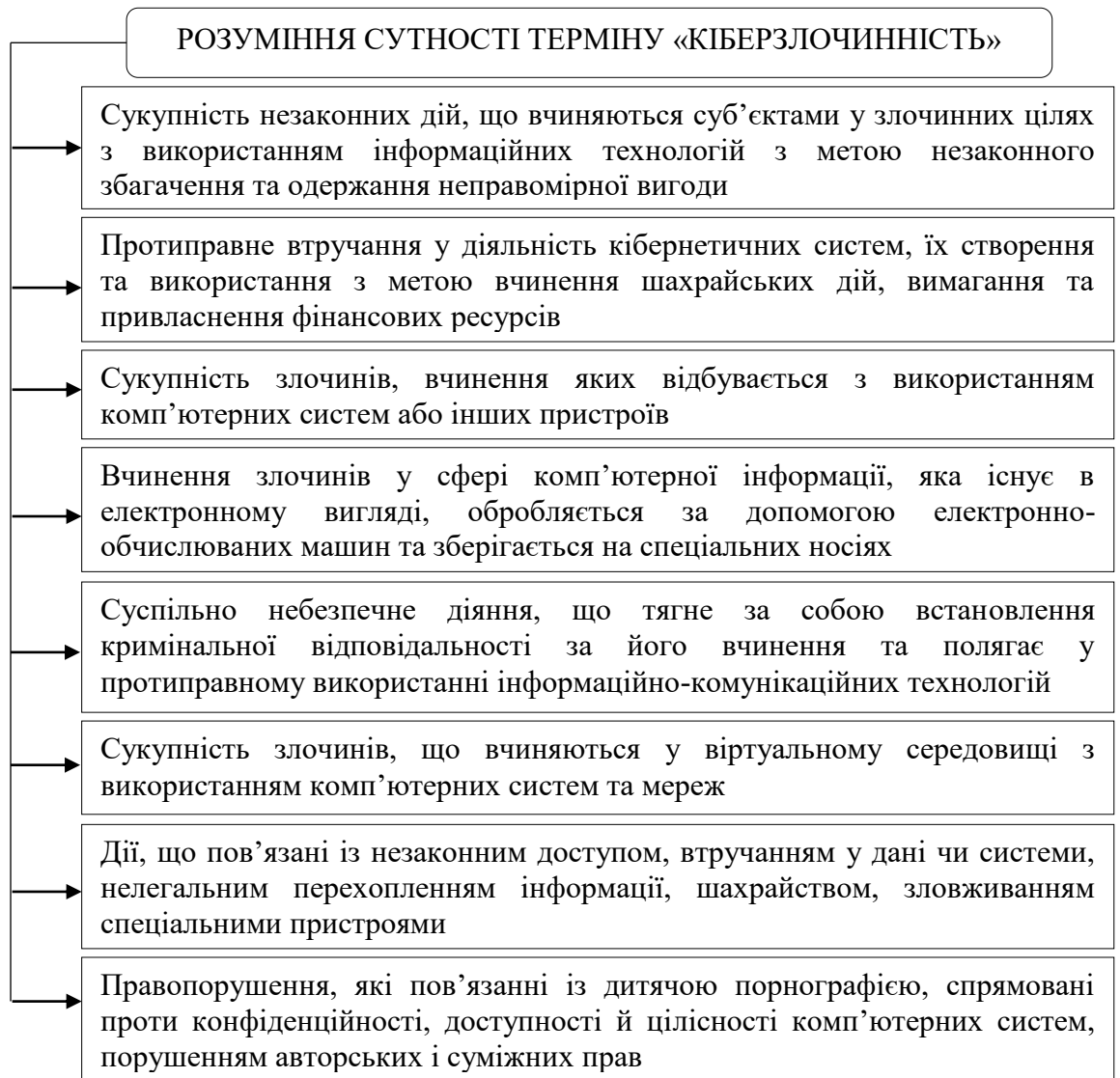


Рис. 1.3. Основні підходи до визначення сутності кіберзлочинності

Джерело: сформовано автором за даними: [14]

Спільними ознаками при визначенні сутності кіберзлочинності можна вважати те, що злочини у кіберпросторі вчиняються із усвідомленням протиправності даних злочинних діянь та, безумовно, спрямовані на одержання неправомірної вигоди та на власне збагачення.

Н. Никончук та О. Маслова [15, с. 203] кіберзлочинність визначають як складне соціальне явище, що являє собою зумисний невмотивований вплив, який передбачає використання мережі Інтернет та інформацію, що знаходиться в комп'ютерних системах, програмах та даних, а також вчиняється особою або групою осіб та становить небезпеку. При цьому

науковці акцентують увагу на неконтрольованості кіберзлочинності та на складності для правоохоронних органів у виявленні кіберзлочинів через їх транснаціональний характер.

У розумінні О. Таран та В. Гавловського [16, с. 195] кіберзлочинність трактується як одне із небезпечних суспільних явищ, що має умисний характер та проявляється у вчиненні протиправних діянь у кіберпросторі або з його використанням. Водночас, науковці дійшли висновку про складність оцінювання рівня кіберзлочинності в країні, оскільки виявили, що існуючі механізми статистичних спостережень за даним деструктивним явищем є неефективними та не дозволяють визначити реальну кількість вчинених кіберзлочинів, структуру кіберзлочинності та стан криміногенної ситуації на національному й регіональному рівнях.

З позиції суб'єктивізму трактує сутність кіберзлочинності Я. Неділько [17, с. 54; 18], який встановив, що кіберзлочинність – це умисні дії, які вчиняються свідомо особою-злочинцем, що посягають на суспільні інтереси, та використовують віртуальне кіберсередовище з метою одержання неправомірної вигоди.

Водночас, необхідно зазначити, що кіберзлочинність є достатньо новим видом економічної злочинності, а її розвиток характеризується поетапністю появи кіберзлочинів. На рис. 1.4 пропонуємо відобразити характеристику таких етапів розвитку кіберзлочинності, запропоновану О. Бодуновою [19, с. 146].



Рис. 1.4. Основні етапи розвитку кіберзлочинності

Джерело: сформовано автором за даними: [19, с. 146]

Як бачимо, розвиток кіберзлочинності охоплює чотири етапи та проходить шлях від її появи як соціально небезпечного явища до проникнення в усі сфери суспільного життя, що свідчить про швидку динаміку її розвитку. При цьому кіберзлочинність передбачає вчинення значного спектру кіберзлочинів, класифікація яких передбачена Конвенцією Ради Європи про кіберзлочинність [20], відповідно до якої виокремлюється декілька груп і видів кіберзлочинів, які систематизуємо на рис. 1.5.

Відповідно до положень Конвенції Ради Європи про кіберзлочинність виокремлюють чотири групи кіберзлочинів, кожен із яких становить небезпеку для держави і суспільства.



Рис. 1.5. Класифікація кіберзлочинів

Джерело: сформовано автором за даними: [20]

Проте, даний перелік кіберзлочинів не є вичерпним, і доповнюється іншими їх видами. Зокрема, виокремлюють кіберзлочини в залежності від об'єкта посягання, до яких належать кіберзлочини проти державних і суспільних інтересів, економічні кіберзлочини та кіберзлочини проти недоторканості приватної сфери та особистих прав.

Чинним законодавством України кіберзлочинність розглядається як сукупність кіберзлочинів, тобто, суспільно небезпечних умисних винних діянь у кіберпросторі та/або з його використанням [21]. Відповідно до Кримінального кодексу України [22] за вчинення кіберзлочинів передбачена відповідальність згідно норм кримінального законодавства. При цьому, Кримінальний кодекс України [22] виокремлює декілька видів кіберзлочинів, зокрема:

- 1) порушення авторського і суміжних прав;
- 2) шахрайство та встановлення доступу до банківської й комерційної таємниці;
- 3) крадіжки персональних даних, особистої й приватної інформації;

- 4) незаконні дії з документами на переказ;
- 5) крадіжки коштів з банківських рахунків та платіжних карток;
- 6) виготовлення, збут та ввезення на територію країни порнографічних матеріалів;
- 7) ухилення від сплати податків.

Проте, в умовах сучасності сформувалися й так звані нові кіберзлочини, які появилися під впливом інтенсифікації процесів цифрової трансформації. До даної групи кіберзлочинів відноситься проведення несправжніх Інтернет-аукціонів, розсилка спаму (електронних листів), проведення азартних ігор у віртуальному середовищі, кіберсквоттинг, фоункрейкинг, камкординг, кардшаринг та створення комп'ютерних вірусів. При цьому, поява нових видів кіберзлочинів стимулює інтенсифікацію процесів розвитку кіберзлочинності та обумовлює необхідність пошуку способів протидії даному деструктивному явищу.

В даному контексті, слухним є зауваження М. Фішеркеллера [23], який стверджує, що боротьба із кіберзлочинністю повинна бути налагоджена на міжнародному рівні, а кожна із країн має долучатися до світового співтовариства та вживати заходів щодо недопущення, попередження та запобігання кіберзлочинності, адже окремі країни умисно застосовують спеціальні коди з метою нанесення шкоди іншим країнам, що ставить під загрозу ефективність існуючих механізмів протидії кіберзлочинності на світовому рівні.

Очевидно, що проблема протидії кіберзлочинності постійно загострюється, а на пошуки дієвих методів боротьби із нею виділяються значні ресурси. Однак, варто визнати, що досягнути бажаних результатів досі не вдалося, оскільки поява нових видів кіберзлочинів засвідчує інтенсифікацію розвитку даного явища, а не ефективність боротьби з нею.

Якщо проаналізувати існуючі наукові підходи до обґрунтування доцільності й об'єктивності застосування різних способів боротьби з

кіберзлочинністю, то можна їх виокремити у декілька груп, які узагальнено на рис. 1.6.



Рис. 1.6. Способи протидії кіберзлочинності

Джерело: сформовано автором за даними: [24]

Як бачимо, основні способи протидії кіберзлочинності зосереджені першочергово на посиленні відповідальності за вчинення кіберзлочинів та на налагодження міжвідомчої й міжнародної взаємодії у сфері боротьби із економічною злочинністю. Проте, їх обмеженість засвідчує потребу у встановленні єдиних правил поведінки в кіберпросторі та посиленні правового регулювання відносин у віртуальному середовищі, що в сукупності дозволить підвищити ефективність боротьби з кіберзлочинністю.

Отже, проведені дослідження кіберзлочинності як небезпечного соціально-економічного явища, дозволяють визначити її сутність, основні види та окреслити способи протидії. Встановлено, що кіберзлочинність трактується як сукупність злочинів, що вчиняються у змодельованому за допомогою комп'ютера інформаційному просторі, в якому систематизовані та зберігаються відомості про процеси, явища та факти, дані про осіб в процесі руху по локальних і глобальних комп'ютерних системах.

Висновки до розділу 1

1. Інтенсифікація процесів тінізації економіки та значне накопичення нелегальних капіталів обумовлює необхідність їх узаконення та залучення до офіційного обігу, що потребує легалізації (відмивання) доходів, одержаних злочинним шляхом. Встановлено, що в умовах сучасності активізувався розвиток легалізаційних процесів, а легалізація (відмивання) грошових коштів, майна та інших активів трансформувалася в один із найнебезпечніших економічних злочинів, набула глобальних масштабів та потребує розроблення ефективних механізмів запобігання та протидії.

2. Виявлено значний дестабілізуючий вплив легалізаційних процесів на національну економіку та суспільство, який проявляється у появі вагомих диспропорцій соціально-економічного розвитку країни, у зростанні соціальної нестабільності та соціальної напруги, в посиленні фінансово-економічної невизначеності та макроекономічної кризи.

3. З'ясовано, що процеси цифровізації економіки і суспільства спричинили стрімкий розвиток кіберзлочинності, яка визначається як складне та небезпечне соціально-економічне явище, що проявляється у вчиненні протиправних діянь із використанням кіберпростору, які спрямовані на збагачення та одержання неправомірної вигоди за рахунок використання інформаційних технологій і комп'ютерних систем, вчинення шахрайських дій та несанкціонованого використання інформації й персональних даних.

4. Доведено складність статистичних оцінювань стану та тенденцій зміни кіберзлочинності в країні, що обумовлено відсутністю належного методичного інструментарію оцінювання рівня кіберзлочинності, визначення кількості кіберзлочинів, а також дослідження їх структури.

РОЗДІЛ 2

АНАЛІЗ СТАНУ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ ТА ПРОБЛЕМ ЇЇ ПРОТИДІЇ В КОНТЕКСТІ ЗАПОБІГАННЯ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ ЗЛОЧИННИМ ШЛЯХОМ

2.1. Сучасний стан кіберзлочинності в Україні

Посилення процесів цифровізації економіки й суспільства обумовлюють виникнення нових ризиків, загроз та небезпек, які проявляються у дестабілізуючому впливі на процеси і явища, що відбуваються із їх використанням. В умовах сучасності істотно загострилися проблеми залучення інноваційних інформаційних технологій в механізми регулювання фінансово-економічних відносин, внаслідок чого актуалізувалася потреба використання віртуального середовища з метою здійснення відповідних операцій фінансового характеру. Більше того, кіберпростір перетворився на зручний плацдарм для здійснення діяльності не лише в межах національної економіки, а й на глобальному рівні.

Однак, поряд із позитивними аспектами розвитку інформаційно-комунікаційних та комп'ютерних технологій виникають проблеми використання віртуального середовища у злочинних цілях, адже кіберпростір надає безмежні можливості для діяльності організованої злочинності та вчинення злочинів, оскільки забезпечується високий ступінь конфіденційності та захисту. Зважаючи на зазначене, можна стверджувати, що сучасне віртуальне середовище сприяє розвитку кіберзлочинності, як одного із небезпечних напрямів кримінальної діяльності, а оскільки інноваційні технології активно використовуються для вчинення злочинних діянь в національній економіці та, зокрема, у фінансово-банківській системі, що пов'язані із узаконенням нелегально одержаних тіньових капіталів, то

актуалізується потреба у її емпіричних оцінюваннях в контексті протидії легалізаційним процесам.

Якщо провести дослідження загального стану кіберзлочинності в Україні, то можна виявити зростаючі тренди щодо кількості кіберзлочинів, які виявлені в Україні у період 2017–2023 рр. (рис. 2.1). При цьому, особливо значне зростання такого виду злочинних посягань зафіксовано у 2023 р. до 61391 злочинів за рік.

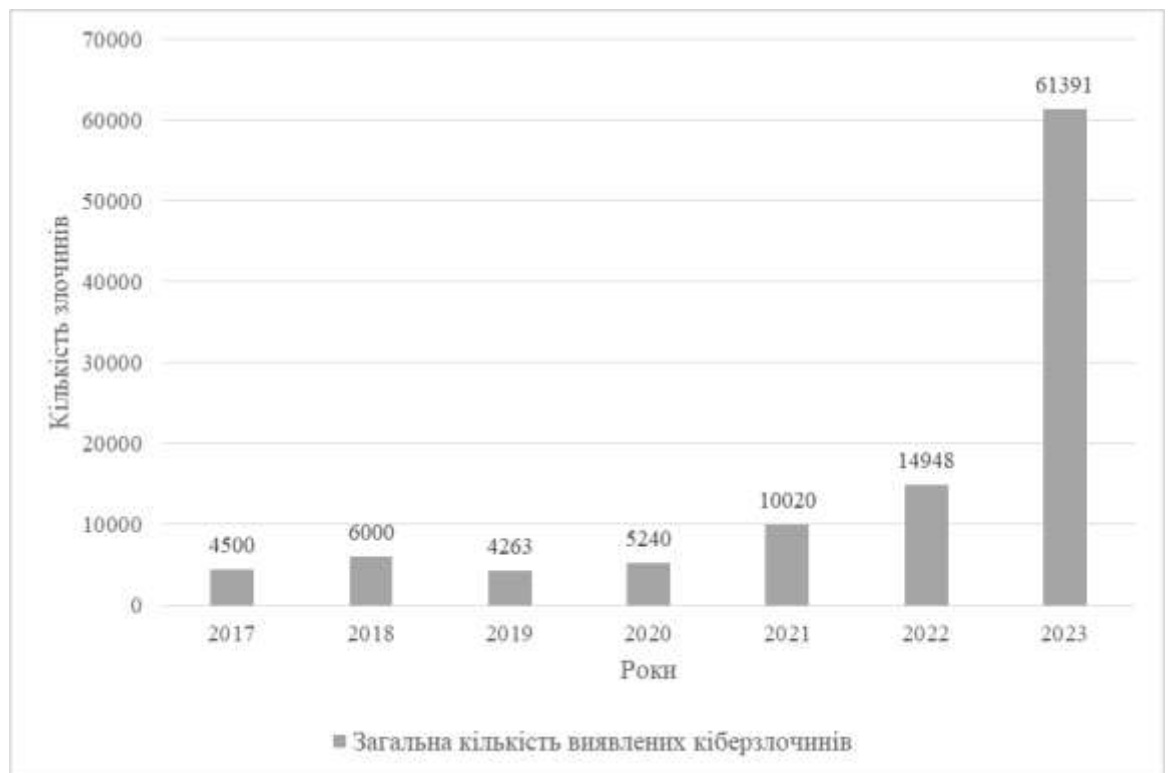


Рис. 2.1. Стан та динаміка зміни кількості кіберзлочинів, виявлених в Україні у 2017–2023 рр.

Джерело: сформовано автором за даними: [25, с. 13; 26, с. 14; 27, с. 6; 28, с. 12; 29, с. 16; 30, с. 11; 31, 9–10]

За звітними даними Національної поліції України в країні впродовж усього аналізованого періоду спостерігається поступове посилення кіберзлочинності, а особлива її активізація припадає на періоди суспільно-політичної та фінансово-економічної нестабільності. Зокрема, найбільш

гостра фаза зростання кількості кіберзлочинів припадає на період поширення пандемії COVID-19 та запровадження значних карантинних обмежень, що обумовило зниження рівня соціальної активності населення та активізувало процеси переходу до здійснення електронних розрахунків із використанням електронних та комп'ютерних систем. Відповідно, за період 2020–2021 рр. кількість кіберзлочинів зросла із 4263 випадків у 2019 р. до 10020 випадків у 2021 р.

Ще більш негативною характеризується ситуація щодо активізації кіберзлочинності у період повномасштабного вторгнення російської федерації на територію України та розв'язання нею невиннованої війни. У 2022 р. під впливом чинників війни та посилення фінансово-економічної й суспільно-політичної нестабільності кількість кіберзлочинів зросла до 14948 випадків за рік, а у 2023 р. до безпрецедентного значення у 61391 кіберзлочин за рік, яке є катастрофічним для України та вимагає негайного прийняття управлінських рішень щодо розроблення ефективних механізмів протидії даному деструктивному явищу.

При цьому, встановлено, що найбільшу питому вагу у загальній структурі кіберзлочинів мають злочини, що пов'язані із онлайн шахрайством. Емпіричні дослідження їх стану та тенденцій зміни впродовж 2017–2023 рр. відобразимо на рис. 2.2.

Як бачимо, в Україні стрімко зростає кількість злочинів, що пов'язані із онлайн шахрайством. При цьому, значне зростання значення аналізованого показника також спостерігається в період з 2021 р. по 2023 р. та катастрофічна ситуація у 2023 р. Так, у 2017 р. даних щодо кількості кіберзлочинів, пов'язаних із онлайн шахрайством зафіксовано не було, у 2018 р. кількість таких злочинних діянь становила 1598 злочинів. У 2019 р. зафіксовано позитивний низхідний тренд, що свідчить про зменшення кількості кіберзлочинів, пов'язаних із онлайн шахрайством до 744 випадків. Однак, починаючи із 2020 р. спостерігається стійкий тренд до зростання, а

саме із 1355 кіберзлочинів у 2020 р. до 45748 кіберзлочинів у 2023 р. (+44393 злочини у порівнянні із 2020 р.).

Очевидно, що така ситуація вимагає негайного реагування та посилення заходів протидії кіберзлочинності в Україні, адже за рахунок протиправних діянь у віртуальному середовищі зростають темпи накопичення тіньових капіталів, які потребують узаконення та легалізації.



Рис. 2.2. Стан та динаміка зміни кількості кіберзлочинів, пов'язаних із онлайн шахрайством, що виявлені в Україні у 2017–2023 рр.

Джерело: сформовано автором за даними: [25, с. 13; 26, с. 14; 27, с. 6; 28, с. 12; 29, с. 16; 30, с. 11; 31, 9–10]

Серед найбільш поширених видів та схем онлайн шахрайства працівниками органів Національної поліції визнано:

1) фішинг (створення фішингових сайтів з метою одержання конфіденційних даних шляхом копіювання дизайну банківських платформ, маркетплейсів, сервісів обміну валют, урядових ресурсів, служб доставки та ін.);

2) заміна SIM-карти (зловмисники декілька разів телефонують абоненту та схиляють його перетелефонувати їм, після чого замовляють в оператора послугу з відновлення SIM-карти, маючи при цьому можливість ідентифікації абонента через ідентифікацію номерів, з яких та на які надходили дзвінки, а також перераховують жертві на мобільний рахунок незначні суми коштів, щоб володіти інформацією про дату останнього поповнення рахунку);

3) схема «друг просить у борг у месенджері» (у соцмережі надходять повідомлення із проханням позичити певну суму коштів);

4) продаж неіснуючих товарів (фейковий Інтернет-магазин або псевдопродавець просить передоплату за придбаний товар, однак зазначеного товару не надсилає).

Іншим достатньо поширеним видом кіберзлочинності в Україні є кіберзлочини, які вчинені у банківській сфері держави. Результати проведених досліджень стану та динаміки зміни кількості кіберзлочинів, вчинених у банківській сфері, які виявлені в Україні у 2017–2023 рр. (рис. 2.3), дають підстави стверджувати, що в країні не має стійкої тенденції до зростання або зниження кількості даного виду злочинних посягань. Швидше констатується циклічний характер вчинення кіберзлочинів у банківській сфері.

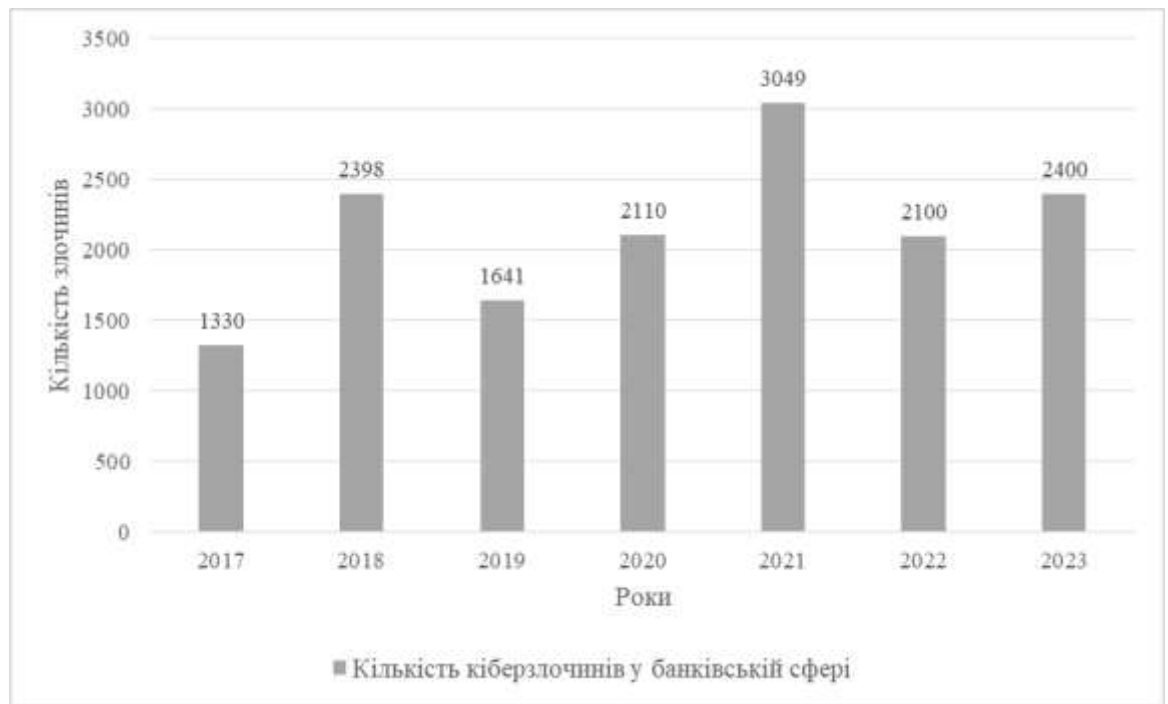


Рис. 2.3. Стан та динаміка зміни кількості кіберзлочинів, вчинених у банківській сфері, які виявлені в Україні у 2017–2023 рр.

Джерело: сформовано автором за даними: [25, с. 13; 26, с. 14; 27, с. 6; 28, с. 12; 29, с. 16; 30, с. 11; 31, 9–10]

Зокрема, варто відзначити декілька основних кризових періодів, а саме 2018 р. та 2021 р., в яких зафіксовано найвищі значення щодо кількості вчинених кіберзлочинів – 2398 злочини у 2018 р. та 3049 злочинів у 2021 р. Після посилення антилегалізаційного законодавства України та паралельно із посиленням вимог до суб'єктів первинного фінансового моніторингу щодо належної перевірки даних, ідентифікації й верифікації їх клієнтів та вжиття відповідних заходів щодо недопущення проявів використання банківських установ і систем з метою легалізації (відмивання) доходів, одержаних злочинним шляхом, кількість кіберзлочинів, вчинених у банківській сфері, знизилася. Проте, у 2023 р. на фоні загального зростання кількості кіберзлочинів кількість злочинних діянь у банківській сфері також має тенденцію до зростання.

Більше того, вчинення кіберзлочинів у банківській сфері тісно корелює із параметрами кіберзлочинності у сфері комп'ютерних систем. Якщо проаналізувати основні тенденції стану та динаміки зміни кількості кіберзлочинів, вчинених у сфері комп'ютерних систем, які виявлені в Україні у 2017–2023 рр. (рис. 2.4), то можна прослідкувати аналогічні закономірності, що й у попередніх дослідженнях. Зокрема, значне зростання кількості кіберзлочинів, вчинених у сфері комп'ютерних систем, спостерігається у період 2017–2019 рр. із 1076 злочинів за рік до 1494 злочинів у 2019 р. У 2020 р. зафіксовано незначне зниження значення зазначеного аналізованого показника до 1461 злочину.

Проте, вже у 2021 р. під впливом карантинних обмежень, пов'язаних із поширенням пандемії COVID-19 та активізацією процесів здійснення фінансових операцій і розрахунків у віртуальному середовищі, кількість кіберзлочинів, вчинених у сфері комп'ютерних систем, різко збільшилася до 1981 випадка. Незначне послаблення та позитивний тренд спостерігається у 2022 р. – виявлена кількість кіберзлочинів, вчинених у сфері комп'ютерних систем, становить 1300 випадків, однак, у 2023 р. знову він має тенденцію до зростання, а значення аналізованого показника піднялося до позначки у 1900 кіберзлочинів.

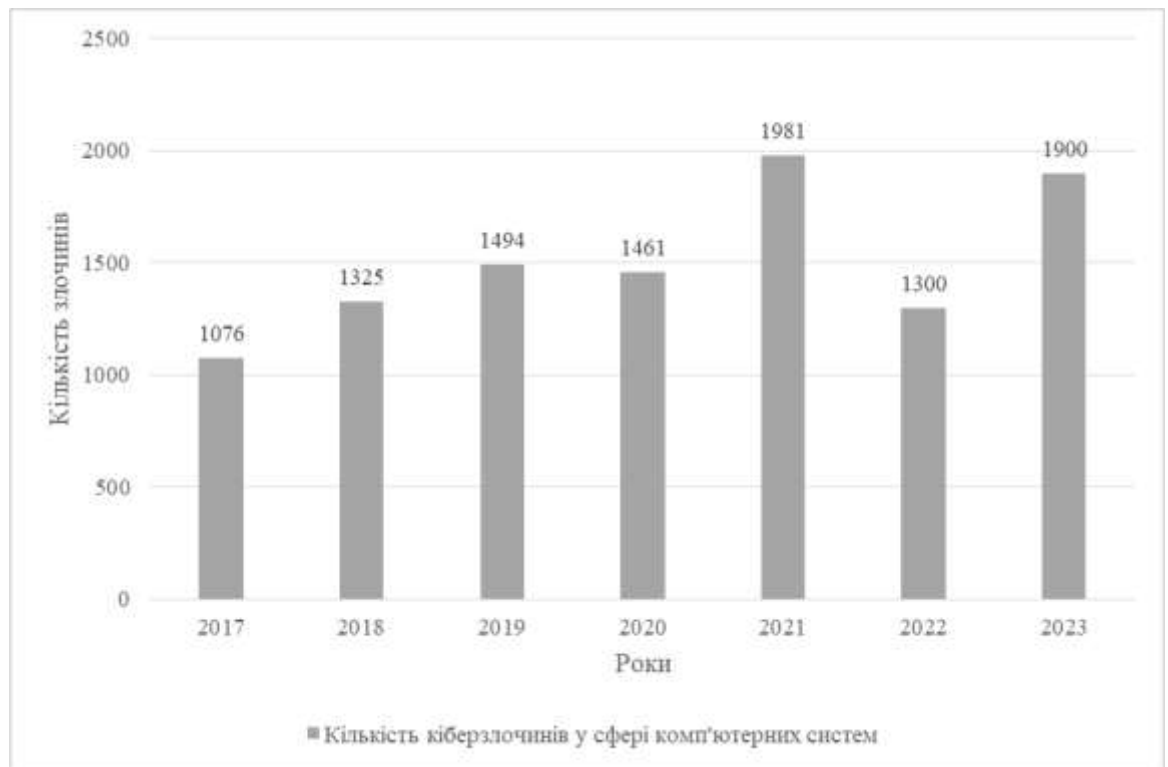


Рис. 2.4. Стан та динаміка зміни кількості кіберзлочинів, вчинених у сфері комп'ютерних систем, які виявлені в Україні у 2017–2023 рр.

Джерело: сформовано автором за даними: [25, с. 13; 26, с. 14; 27, с. 6; 28, с. 12; 29, с. 16; 30, с. 11; 31, 9–10]

Очевидно, що така ситуація щодо масштабного зростання кількості вчинених в Україні впродовж 2017–2023 рр. кіберзлочинів викликає неабияке занепокоєння та становить істотну загрозу інтересам держави і суспільства, знижуючи при цьому рівень безпеки. Активізація кіберзлочинності та транснаціональний характер такого роду протиправних посягань свідчать про необхідність ведення боротьби з даним деструктивним явищем не лише на рівні однієї країни, а виникає потреба у консолідації зусиль усієї міжнародної спільноти.

Варто зауважити, що певні напрацювання в даному керунку уже зроблені, про що свідчить розроблення методології розрахунку Глобального індексу кібербезпеки, який охоплює комплекс показників, що характеризують стан та тенденції зміни кіберпростору та процесів, що

відбуваються у ньому. Зокрема даний міжнародний показник проводить дослідження стану кібербезпеки кожної країни за такими критеріями як:

- 1) спроможність вчасно виявляти кіберзагрози та кіберризики;
- 2) формування системи забезпечення кібербезпеки;
- 3) розроблення механізмів стимулювання розвитку освіти у кіберпросторі;
- 4) формування й реалізація програм посилення кіберграмотності населення.

Результати дослідження значень України за показником Глобального індексу кібербезпеки за період із 2017 р. по 2023 р. вважаємо за доцільне систематизувати на рис. 2.5.

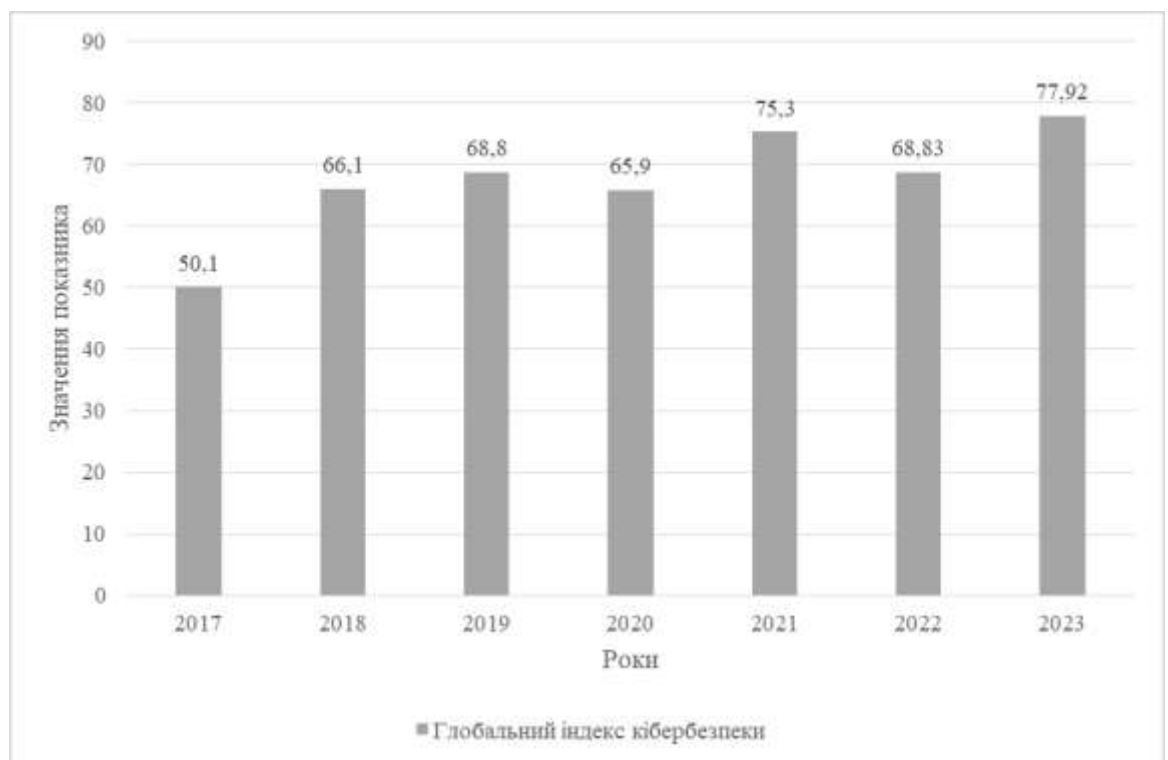


Рис. 2.5. Стан Глобального індексу кібербезпеки в Україні та динаміка його зміни у 2017–2023 рр.

Джерело: сформовано автором за даними: [32–38]

Як засвідчують одержані результати, в країні Глобальний індекс кібербезпеки не має сталого значення, а коливається від 50,1 у 2017 р. до 77,92 у 2023 р. Такі тенденції говорять про те, що відповідні заходи протидії кіберзагрозам та кіберризикам розроблені та запроваджені. Однак, зважаючи на достатньо низьке значення аналізованого показника, можна констатувати їх низьку ефективність. Більше того, вкрай критичне зростання кількості кіберзлочинів у 2023 р. доводить необхідність перегляду існуючих механізмів протидії кіберзлочинності та забезпечення кібербезпеки та їх удосконалення.

Таким чином, проведені дослідження проблемних аспектів аналізу стану кіберзлочинності в Україні дозволяють встановити, що в умовах сучасності кіберзлочинність набула нечуваних масштабів, продовжує інтенсифікацію свого розвитку, залучає новий спектр інноваційних схем вчинення кіберзлочинів та широко використовується не лише для накопичення неправомірно одержаних грошових коштів, майна та інших активів, а й виявляється інструментом легалізації тіньових капіталів.

2.2. Оцінювання обсягів легалізації доходів, отриманих у сфері кіберзлочинності

Легалізація (відмивання) доходів, одержаних злочинним шляхом, виявляється однією із вагомих проблем соціально-економічного розвитку України та потребує розроблення ефективних механізмів її швидкого вирішення. Однак, для того, щоб забезпечити протидію легалізаційним процесам, необхідним виявляється проведення повних, об'єктивних та достовірних оцінювань обсягів легалізації доходів в цілому та виокремлення в їх структурі тих, що отримані у сфері кіберзлочинності від вчинення кіберзлочинів.

Проведені дослідження щодо виявлення загальних тенденцій у сфері протидії легалізації (відмивання) злочинно отриманих капіталів в Україні за період 2017–2023 рр. дозволяють встановити неоднозначний характер аналізованої проблематики. Стан та динаміка зміни обсягів коштів, отриманих злочинним шляхом, що легалізовані в Україні (рис. 2.6) свідчать про те, що легалізаційні процеси стабільно розвиваються, а суми виявлених легалізованих активів доводять вагомість та небезпеку даного деструктивного явища.

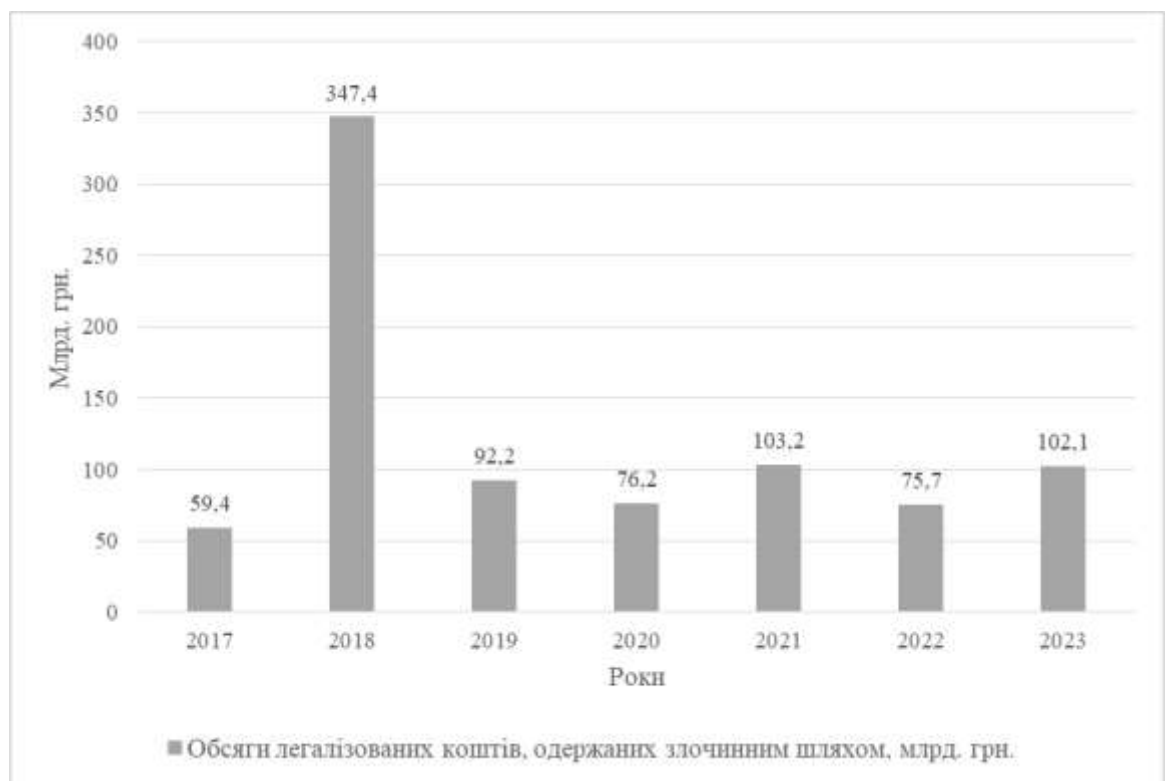


Рис. 2.6. Стан та динаміка зміни обсягів коштів, отриманих злочинним шляхом, що легалізовані в Україні у 2017–2023 рр.

Джерело: сформовано автором за даними: [39, с. 8; 40, с. 8; 41, с. 25; 42, с. 27; 43, с. 6; 44, с. 30; 45, с. 35]

Аналізуючи показники, які відображають стан та динаміку зміни обсягів коштів, отриманих злочинним шляхом, що легалізовані в Україні, можна стверджувати, що найвищі суми зафіксовані у 2018 р. – 347,4 млрд.

грн. Подальші періоди позиціонують дещо нижчі показники, однак, вони залишаються вагомими. З одного боку, це обумовлено посиленням антилегалізаційного законодавства, внаслідок чого злочинна діяльність, пов'язана із відмиванням та узаконенням тіншових капіталів набула менших темпів, однак, характеризується виникненням нових схем та методів легалізаційної діяльності. З іншої сторони, така протиправна діяльність поступово трансформувалася у кіберпростір, де існує високий рівень захисту даних та присутній значний ступінь конфіденційності, внаслідок чого виявлення злочинних діянь, пов'язаних із легалізацією (відмиванням) доходів, майна і активів, виявляється надскладним завданням для правоохоронних органів та спеціалізованих установ.

Очевидно, що значна робота щодо запобігання та протидії легалізаційним проявам ведеться як на національному, так і на міжнародному рівні. Зокрема, Україна удосконалила законодавче й нормативно-правове забезпечення у сфері антилегалізаційної боротьби. Більше того, в країні успішно працює низка спеціалізованих органів, які займаються виявленням, попередженням та протидією легалізації (відмиванню) доходів, одержаних злочинним шляхом, а саме:

- 1) Бюро економічної безпеки України;
- 2) Державна податкова служба;
- 3) Органи прокуратури;
- 4) Національна поліція України;
- 5) Служба безпеки України;
- 6) Державне бюро розслідувань;
- 7) Національне антикорупційне бюро України.

При цьому, усі зазначені спеціалізовані органи тісно співпрацюють із Державною службою фінансового моніторингу України та в межах своїх компетенцій розробляють та реалізують комплекс заходів антилегалізаційної боротьби.

Проведені емпіричні дослідження щодо виявлення показників та параметрів взаємодії Державної служби фінансового моніторингу України із правоохоронними й розвідувальними органами вважаємо за доцільне систематизувати на рис. 2.7.

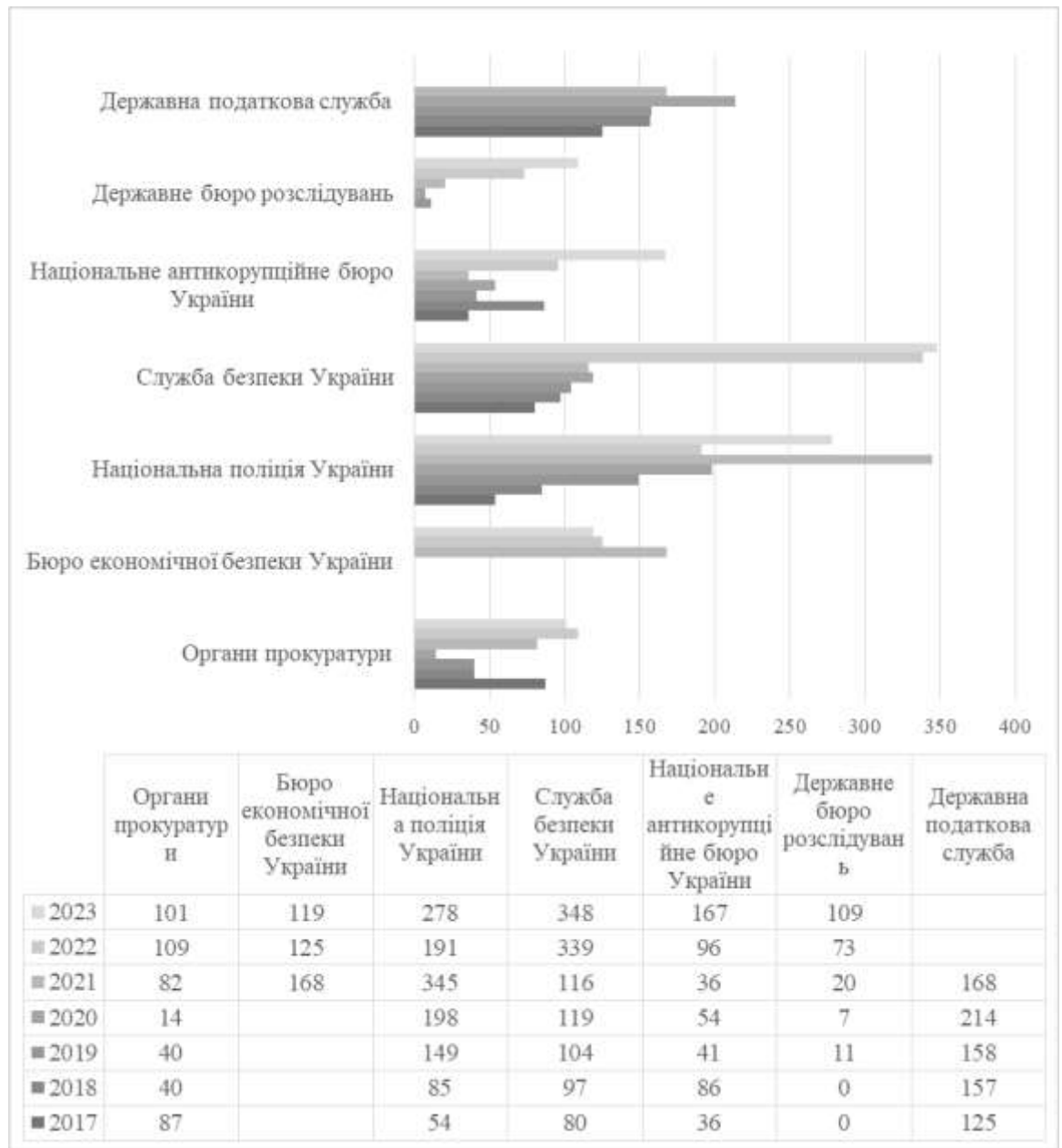


Рис. 2.7. Стан та динаміка зміни кількості матеріалів, переданих Державною службою фінансового моніторингу України до правоохоронних органів у 2017–2023 рр.

Джерело: сформовано автором за даними: [39, с. 8; 40, с. 8; 41, с. 25; 42, с. 27; 43, с. 6; 44, с. 30; 45, с. 35]

Водночас, зазначимо, що найбільша кількість направлених Державною службою фінансового моніторингу України матеріалів, що сформовані за результатами проведених фінансових розслідувань, відмічається до органів Національної поліції України, Служби безпеки України та до Державної податкової служби.

Детальна характеристики стану та динаміки зміни кількості матеріалів, переданих Державною службою фінансового моніторингу України до правоохоронних органів у 2017–2023 рр. дозволяє констатувати, що до 2021 р. найбільшу кількість узагальнених матеріалів, що містять ознаки підозрілих фінансових операцій, які пов'язані із легалізаційними процесами, спеціально уповноваженим органом направлено до Служби безпеки України (в середньому 80–119 справ щорічно) та до Національної поліції України (в середньому 54–345 справ щорічно). Однак, у 2022 р. та 2023 р. тенденції дещо змінилися, зокрема, до органів Національної поліції було направлено 191 матеріал, що на 154 матеріали менше, ніж у 2021 р. Натомість, у відношенні щодо взаємодії із Службою безпеки України зафіксовано зростаючий тренд. Більше того, аналізуючи показники в розрізі усіх видів правоохоронних органів відмічається зростання показників щодо взаємодії Держфінмоніторингу із усіма правоохоронними органами.

Окремо, варто відмітити, що до 2021 р. Державна служба фінансового моніторингу значну кількість матеріалів передавала до Державної податкової служби України, проте, за результатами роботи спеціально уповноваженого органу у 2022 р. та 2023 р. такі дані не узагальнювалися та не включені до звітних документів.

Напротивагу, активна й тісна взаємодія спостерігається між Держфінмоніторингом та Бюро економічної безпеки – новим органом, діяльність якого спрямована на ведення антилегалізаційної боротьби, що створений у 2021 р. Зокрема, у 2021 р. до даної державної структури було

направлено 168 матеріалів справ, у 2022 р. – 125 матеріалів справ та у 2023 р. – 119 матеріалів справ.

Позитивної оцінки заслуговує й взаємодія Держфінмоніторингу із органами прокуратури, оскільки її показники свідчать про зростання кількості опрацьованих та переданих матеріалів справ із 87 у 2017 р. до 101 справи у 2023 р.

Аналогічні тенденції можна відмітити й щодо співпраці із Державним бюро розслідувань, кількість матеріалів справ переданих для опрацювання ним різко зросло із 11 у 2019 р. до 109 матеріалів у 2023 р.

Що стосується ефективності протидії легалізаційним процесам у сфері корупції, то тут також спостерігаються позитивні зрушення, про що свідчить зростання показників щодо кількості матеріалів, переданих Державною службою фінансового моніторингу України до Національного антикорупційного бюро, а саме із 36 справ у 2017 р. до 167 справ у 2023 р.

Очевидно, що така ситуація у сфері протидії легалізаційним процесам є позитивною, однак, на фоні різкого й масштабного зростання загальної кількості злочинів, пов'язаних із легалізацією (відмиванням) доходів, одержаних злочинним шляхом, та кількості кіберзлочинів, зокрема, вона говорить не лише про підвищення ефективності антилегалізаційної боротьби, а й про поглиблення поширеності даного виду злочинних діянь.

При цьому, варто зазначити, що значна частка грошових коштів, майна та інших активів, які отримані внаслідок незаконної діяльності, що здійснювалася у кіберпросторі, готувалися до легалізації із застосуванням різних інструментів, зокрема, шляхом надання фінансової допомоги, здійснення міжнародних переказів, операцій із готівковими коштами, а також через використання платіжних карток, товарів і послуг.

Результати проведених ґрунтовних досліджень дозволили встановити, що найбільш часто використовуваними схемами здійснення злочинних діянь, пов'язаних із легалізацією тіньових капіталів, що одержані від вчинення кіберзлочинів, є:

- 1) шахрайство у сфері заволодіння коштами підприємств-нерезидентів;
- 2) несанкціоноване заволодіння активами шляхом незаконного списання коштів підприємств-нерезидентів;
- 3) використання дистанційного керування з метою незаконного списання коштів із банківських рахунків.

Отже, проведені дослідження щодо виявлення та оцінювання обсягів легалізації доходів, отриманих у сфері кіберзлочинності, дають підстави стверджувати, що даний вид злочинних діянь спричинює значні втрати державного бюджету через узаконення неправомірно одержаних капіталів, які отриманні злочинним шляхом із використанням кіберпростору.

Висновки до розділу 2

1. Доведено, що в Україні загострилася проблема поширення кіберзлочинності та спостерігається інтенсифікація процесів виникнення інноваційних схем вчинення кіберзлочинів, загальна кількість яких станом на 2023 р. становила 61391 злочин, що є загрозливим значенням для розвитку національної економіки й суспільства. Встановлено взаємозалежність та взаємообумовленість зростання кількості кіберзлочинів від посилення соціально-економічної та суспільно-політичної криз.

2. Виявлено зростаючі тренди щодо збільшення кількості кіберзлочинів, пов'язаних із онлайн шахрайством в період запровадження карантинних обмежень зумовлених поширенням пандемії COVID-19 та військовими чинниками сучасності, що обумовлено поступовою трансформацією процесів здійснення фінансових операцій у віртуальне середовище та використанням кіберпростору для проведення фінансово-господарських розрахунків. З'ясовано, що до найбільш вагомих та часто використовуваних схем онлайн шахрайства в Україні відноситься фішинг,

зміна SIM-карти, продаж неіснуючих товарів та схема «друг просить у борг у месенджері».

3. Встановлено, що кіберзлочинність завдає вагомих втрат державному бюджету України, а обсяги легалізації доходів, отриманих у сфері кіберзлочинності постійно зростають. Окреслено основні напрямки та параметри взаємодії Державної служби фінансового моніторингу України із правоохоронними органами та з'ясовано, що найбільшу кількість матеріалів, у яких містяться відомості про підозрілі фінансові операції, передано спеціально уповноваженим органом до Служби безпеки України, органів Національної поліції України, Національного антикорупційного бюро України та до Державної податкової служби України.

РОЗДІЛ 3

УДОСКОНАЛЕННЯ ЗАХОДІВ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

3.1. Стратегічні пріоритети протидії кіберзлочинності

Зростаючі тенденції щодо активізації діяльності злочинців у віртуальному середовищі та стрімке поширення кіберзлочинності засвідчують наявність вагомих проблем у сфері запобігання та протидії даному деструктивному явищу. Очевидно, що кіберзлочинність набула нечуваних досі масштабів та продовжує свій інтенсивний розвиток, що доводиться результатами проведених емпіричних досліджень. Зважаючи на зазначене, можна стверджувати, що існуючі механізми боротьби із кіберзлочинністю є неефективними як на національному, так і на міжнародному рівні та неспроможні протистояти викликам і небезпекам сучасності. Тому, перед державою гостро постає завдання, яке пов'язане із формуванням нової системи заходів протидії кіберзлочинності та забезпечення оптимального рівня захисту інтересів держави і суспільства у кіберсередовищі, адже, в умовах сьогодення активізуються нові виклики у сфері кіберзлочинності, зокрема, відмічається:

- 1) інтенсифікація процесів використання кіберзасобів при вчиненні злочинів у віртуальному середовищі;
- 2) надшвидкий розвиток інформаційно-телекомунікаційних технологій таких як хмарні та квантові обчислення, штучний інтелект, великі дані та 5-G мережі;
- 3) зростання темпів мілітаризації кіберпростору та розвитку кіберзброї;

4) активізація процесів інтенсивної трансформації та виокремлення вагомого сегменту суспільних відносин, що відбуваються у дистанційному режимі з використанням кіберпростору та електронних сервісів;

5) розроблення механізмів запровадження цифрових послуг при взаємодії громадян з державою.

Проведені дослідження засвідчують, що певні напрацювання в зазначеному керунку уже існують, а Україна розуміє вагомість проблематики запобігання і протидії кіберзлочинності, а також зміцненню кібербезпеки держави і суспільства. Зокрема, варто відмітити позитивний ефект від запровадження Стратегії кібербезпеки України [46], в якій визначено основні аспекти створення належних умов для безпечного функціонування кіберпростору та його ефективного використання без порушення інтересів держави і суспільства, запобігання та протидії наявним і потенційним кіберзагрозам, а також визначення пріоритетних напрямків захисту національних інтересів у сфері кібербезпеки.

Іншим нормативно-правовим документом – Планом заходів на 2023–2024 рр. з реалізації Стратегії кібербезпеки України [47] регламентується комплекс спеціальних заходів та перелік завдань, необхідних для запобігання та протидії кіберзлочинності в країні, а також щодо забезпечення достатнього рівня кібербезпеки. Більше того, в документі подано перелік індикаторів дослідження кіберзлочинності та кібербезпеки, а також чіткі терміни реалізації запропонованих заходів.

При цьому, в системі запобігання та протидії кіберзлочинності в Україні можна виокремити декілька основних напрямів реалізації комплексу спеціальних заходів, які запропоновані у Плані заходів на 2023–2024 рр. з реалізації Стратегії кібербезпеки України [47], зокрема:

1) нормативно-правове забезпечення діяльності у сфері безпеки, охорони та захисту кіберпростору;

2) розвиток технологічної складової вітчизняної системи кібербезпеки;

- 3) налагодження співробітництва із міжнародними партнерами;
- 4) формування організаційно-технічної моделі національного кіберзахисту;
- 5) проведення науково-прикладних досліджень у сфері кібербезпеки;
- 6) посилення кіберзахисту об'єктів, що належать до критичної інфраструктури;
- 7) підготовка кадрів у сфері кібербезпеки.

Відповідно, вважаємо, що стратегічні пріоритети забезпечення протидії кіберзлочинності та реалізації Стратегії кібербезпеки України необхідно визначати з урахуванням зазначених напрямів реалізації Стратегії кібербезпеки України. На рис. 3.1 узагальнимо ключові засади формування комплексу заходів щодо забезпечення протидії кіберзлочинності та виконання Стратегії кібербезпеки України, реалізація яких передбачена у стратегічній перспективі.

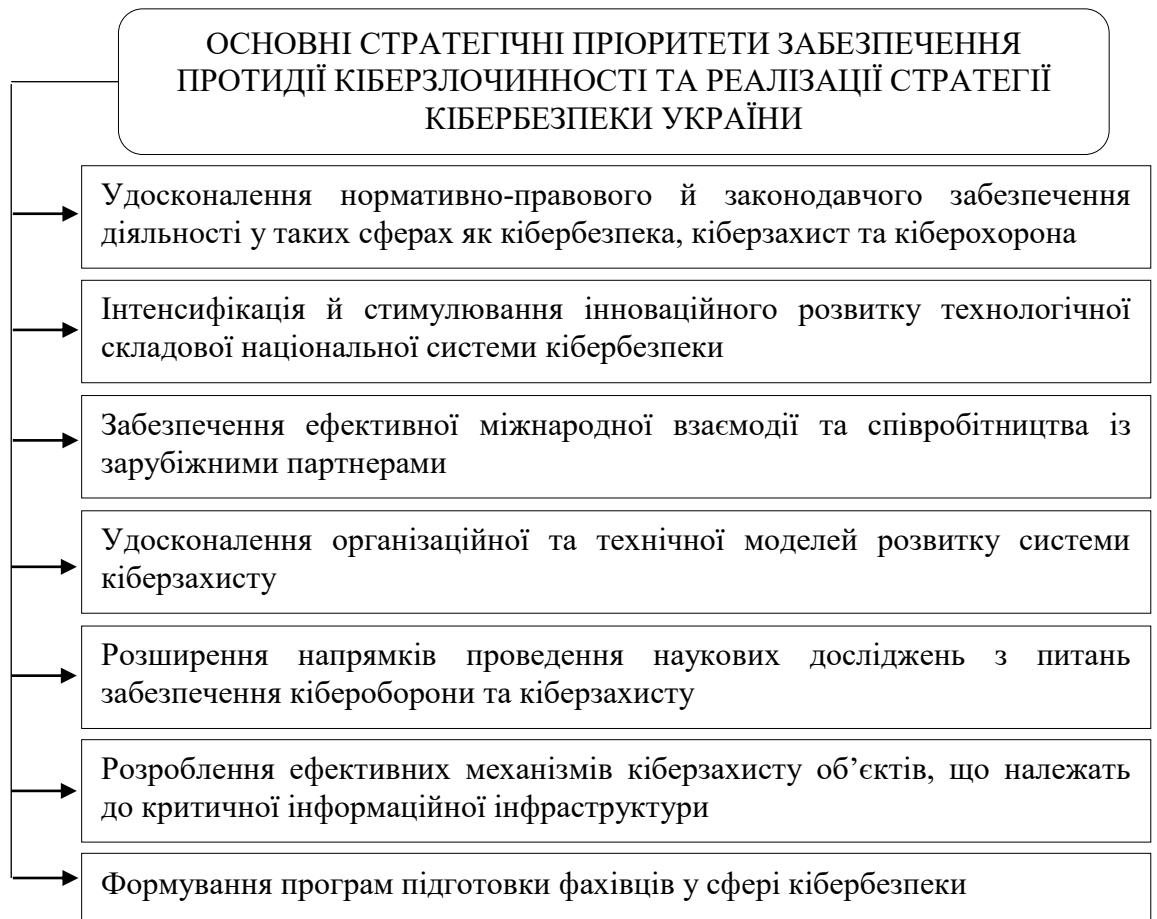


Рис. 3.1. Стратегічні пріоритети забезпечення протидії кіберзлочинності та реалізації стратегії кібербезпеки України

Джерело: власна авторська розробка

Окремо варто звернути увагу на необхідність унормування та законодавчої регламентації функціонування системи індикаторів, за допомогою яких можливим стане проведення оцінювання стану, динаміки зміни та основних тенденцій кібербезпеки, адже, як встановлено, методичного інструментарію оцінювання статистичних показників щодо обсягів, структури та інших параметрів кіберзлочинності в Україні не існує.

Зазначимо, що така система індикаторів орієнтується на затвердженні показників, які різносторонньо висвітлюють реальну ситуацію у кіберпросторі та в системі кібербезпеки. Проведені дослідження доводять, що обґрунтованою виявляється система індикаторів, що охоплює:

- 1) індикатори стану кібербезпеки;

- 2) індикатори розвитку вітчизняної системи кібербезпеки;
- 3) індикатори стану кіберзахисту інформації, об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.

Комплексне дослідження кіберпростору за окресленими індикаторами дозволить виявити ризики і загрози та сформувати ефективну систему їх запобігання та протидії в короткостроковому та довгостроковому періодах.

Крім того, вважаємо за доцільне виокремити й інші стратегічні завдання держави щодо протидії кіберзлочинності й забезпечення достатнього рівня безпеки у віртуальному середовищі, до найбільш вагомих серед яких доцільно віднести:

- 1) формування спеціальної державної системи виявлення кібератак, запобігання і протидії кібертероризму та кібершпигунству з акцентом на посилення захисту об'єктів критичної інформаційної інфраструктури;
- 2) запровадження інноваційних методик обробки й оцінки цифрових даних та формування електронних доказів в контексті удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки на національному рівні;
- 3) удосконалення та посилення механізмів проведення перевірок стану готовності об'єктів критичної інфраструктури до потенційних й можливих кібератак;
- 4) посилення механізмів контррозвідувального захисту ІТ-сфери, сфери електронних телекомунікацій, а також афілійованого з ними середовища забезпечення кібербезпеки;
- 5) створення технологічних можливостей та спеціального програмного забезпечення, спрямованих на створення належних умов для автоматичного виявлення кібератак у режимі реального часу, а також визначення їх пріоритетності та вчасного блокування;
- 6) удосконалення організаційного, кадрового та нормативно-правового забезпечення системи боротьби з кібертероризмом на національному рівні;

7) формування основних засад та реалізація державної політики захисту прав громадян у кіберпросторі;

8) розроблення та запровадження на національному рівні практики проведення інформаційної роз'яснювальної роботи щодо алгоритмів дій громадян у випадку прояву щодо них кібершахрайства та інших кіберзлочинів;

9) розроблення механізмів формування кіберстатистики та методики проведення соціологічних досліджень щодо кіберзагроз, з якими стикається населення;

10) гармонізація вітчизняної санкційної політики із нормами міжнародного підходу до застосування санкцій як відповідь на ведення підривної діяльності у кіберпросторі;

11) розроблення та гармонізація із міжнародними механізмами дипломатичних відносин щодо реалізації економічних дій і обмежувальних заходів у відповідь на злочинну кіберактивність.

Істотно посилить заходи протидії кіберзлочинності в Україні утворення постійно діючої робочої групи, до компетенції якої входять функції взаємодії із провідними світовими провайдерами цифрових послуг та ІТ-компаніями щодо протидії кіберзагрозам та поширенню інформації у кіберсередовищі. Зазначене особливо актуалізується в умовах посилення необхідності розроблення механізмів запровадження цифрових послуг при взаємодії громадян з державою, адже, цифровізація суспільства продовжується та виникають вагомі ризики і небезпеки при переході до надання цифрових послуг.

В даному контексті варто звернути увагу на той факт, що рівень довіри приватного сектору до цифрових послуг, що надаються державою, є достатньо низьким в умовах сьогодення, що пов'язано із насторогами населення та відсутністю дієвих механізмів його інформування державою щодо безпечності і надійності надання таких послуг. Очевидно, що за таких обставин своєчасним та вкрай необхідним виявляється розроблення та

реалізація Загальнодержавної програми кіберграмотності як ефективного державного документу врегулювання проблемних питань підвищення рівня цифрової грамотності громадян України. При цьому, зазначений документ повинен включати певні аспекти набуття населенням широкого спектру цифрових навичок та кіберобізнаності про існування сучасних кіберзагроз, їх видів та небезпеки, які вони спричиняють.

Не менш важливим залишається доцільність розроблення системи проведення аудиту інформаційної безпеки та кібербезпеки, а також методики його проведення, зокрема, й тих об'єктів, що належать до критичної інфраструктури. Однак, дана пропозиція передбачає перепідготовку та підготовку кадрового складу аудиторів, встановлення вимог до їх компетентності, а також атестацію, сертифікацію та підвищення кваліфікації, що додатково обумовлює необхідність розроблення спеціальних програм навчання.

Зважаючи на зазначене, окреслюються тенденції, відповідно до яких можна сформулювати декілька напрямів визначення стратегічних пріоритетів забезпечення кібербезпеки України та протидії кіберзлочинності, а саме:

- 1) захист кіберпростору в інтересах збереження державного суверенітету та сталого розвитку держави і суспільства;
- 2) захист прав, свобод та інтересів населення у кіберпросторі;
- 3) євроінтеграція у сфері кібербезпеки.

Очевидно, що першочергового значення в умовах сучасності при удосконаленні механізмів протидії кіберзлочинності в Україні набуває удосконалення чинного законодавства, зокрема, в частині посилення відповідальності за вчинення кіберзлочинів. Поряд із зазначеним, вважаємо за доцільне обґрунтувати пропозицію розроблення та прийняття Закону України «Про державно-приватне партнерство у сфері кібербезпеки», який дозволить врегулювати проблемні питання щодо визначення форм такого партнерства та методів його здійснення на засадах зміцнення взаємної довіри та допомоги.

Таким чином, результати дослідження можливостей визначення стратегічних пріоритетів протидії кіберзлочинності в Україні дозволяють сформувати певні вектори запобігання та протидії кіберзлочинності в країні та забезпечення достатнього рівня кібербезпеки. На підставі проаналізованого, виявлено необхідність удосконалення чинного законодавства та нормативно-правового забезпечення діяльності у сфері безпеки, охорони та захисту кіберпростору та обґрунтовано необхідність розроблення та прийняття Закону України «Про державно-приватне партнерство у сфері кібербезпеки», а також розроблення системи проведення аудиту інформаційної безпеки і методики його проведення. Встановлено відсутність методичного інструментарію проведення статистичних досліджень стану та динаміки зміни кіберзлочинності в Україні, що потребує законодавчого врегулювання даної проблеми. Обґрунтовано необхідність посилення основних аспектів підвищення кіберграмотності населення, що, своєю чергою, потребує розроблення та реалізації Загальнодержавної програми кіберграмотності населення.

3.2. Міжнародний досвід удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності

Інтенсифікація розвитку кіберзлочинності, поява нових методів та схем вчинення кіберзлочинів та стрімке зростання кількості виявлених кіберзлочинів в Україні в нестійких умовах її розвитку під впливом чинників російсько-української війни обумовлюють необхідність пошуку ефективних механізмів запобігання та протидії даному деструктивному явищу. Очевидно, що активізація кіберзлочинності перебуває у тісному взаємозв'язку із накопиченням нелегально одержаних капіталів і їх легалізація відбувається одномоментно із вчиненням злочинів у кіберпросторі. Тому, поряд із необхідністю протидії кіберзлочинності обумовлюється потреба у

формуванні ефективної системи протидії легалізації доходів, які отримані у сфері кіберзлочинності.

Попередні дослідження свідчать, що злочинна діяльність, пов'язана із кіберзлочинністю та легалізацією (відмиванням) доходів, одержаних злочинним шляхом, тісно пов'язані між собою та в деякій мірі взаємодоповнюються, а оскільки є транснаціональними явищами, то й заходи ефективної боротьби повинні розроблятися із урахуванням світових тенденцій. При цьому, встановлено, що високо розвинуті країни розробили ефективні системи антилегалізаційної боротьби та дієві механізми протидії кіберзлочинності, а країни транзитивного типу є інсайдерами у цій сфері та власними силами не спроможні забезпечити достатній рівень кібербезпеки.

Проблеми боротьби із кіберзлочинністю в Україні існують й особливо загострилися в умовах запровадження спеціального правового режиму воєнного стану та характеризуються відсутністю ефективних механізмів протидії легалізації результатів такої злочинної діяльності. Ситуація поглиблюється складністю відмивання коштів і активів, що одержані у сфері кіберзлочинності, адже вчиняються кіберзлочини на значних територіях з використанням глобальної мережі Інтернет та мають високий рівень анонімності й конфіденційності. Стає очевидним, що Україна потребує адаптації міжнародних практик протидії легалізації коштів, одержаних у сфері кіберзлочинності, до умов її функціонування, тому аналіз та оцінювання світового досвіду удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності, є доцільним та необхідним.

Проведені дослідження існуючих наукових розробок у зазначеній сфері дають підстави стверджувати, що на міжнародному рівні не сформовано єдиний підхід до визначення пріоритетів протидії легалізації (відмиванню) злочинно одержаних коштів та, фактично, в кожній із країн функціонує спеціально уповноважений підрозділ фінансової розвідки, зокрема у США – Департамент посилення боротьби із фінансовою злочинністю, у Канаді такий підрозділ називається Центром аналізу фінансових операцій, у Японії

функціонує Японський офіс фінансової розвідки, а в Греції – Спеціальний комітет боротьби з відмиванням грошей. В окремих країнах, зокрема, у Мексиці створено та здійснює діяльність два державні органи – Генеральний директорат з розслідування транзакцій та Агенство боротьби з відмиванням грошей [48, с. 627]. При цьому, в окремих країнах такі спеціалізовані органи є органами адміністративного типу (США), органами юстиції (Аргентина) та поліцейськими органами (Мексика, Австрія).

Очевидно, що адаптація позитивних міжнародних практик протидії легалізації грошових коштів, майна та активів, що здобуті внаслідок вчинення злочинів у кіберпросторі, до умов функціонування України є складним процесом, що вимагає врахування вітчизняних особливостей розвитку держави і суспільства. Безумовно, основні аспекти використання зарубіжного досвіду повинні узгоджуватися із національною правовою системою, враховувати її особливості та специфікацію та відповідати існуючим спроможностям забезпечення кіберстійкості.

В даному контексті варто відмітити позитивний досвід США щодо забезпечення ефективної протидії як кіберзлочинності, так і інтенсифікації легалізаційних процесів. У США ще у 2001 р. прийнято такий вагомий документ як Стратегія безпеки в кіберпросторі [49], де уніфіковано організаційно-правові аспекти захисту інтересів держави і суспільства у кіберпросторі. Крім того, США власним законодавством передбачили достатньо жорсткі види відповідальності за вчинення кіберзлочинів та за узаконення доходів, що одержані у неправомірний спосіб із використанням кіберпростору.

Ще одним позитивним аспектом протидії легалізації коштів, що одержані у кіберпросторі, який застосовується у США, є високий рівень захисту від кіберзагроз і кібератак. Більше того, в країні сформовано національні стандарти безпеки у кіберпросторі, що дозволяє розробити механізми швидкого виявлення кіберзлочинів та попередження й протидії злочинній діяльності у віртуальному середовищі.

На рівні Європейського Союзу Стратегія кібербезпеки ЄС прийнята у 2013 р., а в Україні такий важливий стратегічний документ ухвалений лише у 2021 р. Очевидно, що така ситуація свідчить про недостатній рівень ефективності протидії економічній злочинності та забезпечення кібербезпеки. Більше того, важливим для України є запозичення позитивних практик формування національної моделі забезпечення кіберзахисту, кібероборони та кібербезпеки, у структурі якої виокремлюється механізм протидії кіберзлочинності.

На міжнародному рівні у сфері протидії легалізації доходів, отриманих у сфері кіберзлочинності, вагому роль відіграє створення спеціально уповноважених органів, до компетенції яких належить реалізація комплексу заходів, спрямованих на запобігання, протидію кіберзлочинності, а також на попередження вчинення кіберзлочинів. Варто відзначити, що такі органи уже створені та успішно функціонують у США, Канаді та в таких європейських країнах як Великобританія, Данія, Швейцарія, Нідерланди, Норвегія, Австрія, Бельгія, Німеччина, Польща та Естонія.

Не зважаючи на достатньо вагомий рівень антилегалізаційної боротьби із узаконенням доходів, одержаних у сфері кіберзлочинності, залишається невирішеною проблема законодавчого врегулювання питань опрацювання електронних доказів вчинення кіберзлочинів. Очевидно, що в даному напрямку ведуться дослідження, однак механізми виявлення та передачі електронних доказів в Україні досі неунормовані, що, на відміну від США, Великобританії та окремих країн Європейського Союзу, становить істотну перешкоду при проведенні відповідних розслідувань злочинних діянь, пов'язаних із легалізацією.

Ще однією проблемою виявляється недосконалість процедури здійснення віддалених обшуків інформаційних ресурсів, адже, їх часте розміщення за межами країни обумовлює неможливість доступу та довготривалість процесів одержаних доказової бази. Щодо даного питання доцільним виявляється розгляд досвіду Франції, яка на міждержавному рівні

налагодила взаємозв'язки та уклала низку спеціальних угод, якими, фактично, усунено кордони між країнами у сфері боротьби із кіберзлочинністю та сформовано механізми державного регулювання відносин, що здійснюються у віртуальному середовищі. Крім того, у Франції налагоджена тісна взаємодія правоохоронних органів із Інтернет-провайдерами, що дозволяє вчасно виявляти кіберризики, запобігати кіберзагрозам та протидіяти небезпекам.

Таким чином, проведені дослідження дозволяють стверджувати, що в зарубіжних країнах, так як і в Україні, існують вагомі проблеми боротьби із кіберзлочинністю, а на міжнародному рівні виокремлюється низка проблемних питань забезпечення кібербезпеки та протидії легалізації результатів злочинної діяльності, акумульованих у кіберпросторі, серед найбільш вагомих із яких виокремлюється:

- 1) відсутність єдиної уніфікованої міжнародної системи заходів реагування на кіберзагрози, кіберризики та кібератаки;

- 2) національні стандарти у сфері протидії кіберзлочинності та забезпечення кібербезпеки й ефективної протидії легалізаційним проявам істотно відрізняються та адаптовані до вітчизняних умов ведення такої боротьби в залежності від норм чинного законодавства у кожній із зарубіжних країн;

- 3) відсутність єдиного спеціалізованого органу боротьби із кіберзлочинністю на рівні країни, а функції такої протидії, здебільшого, покладено на органи поліції.

Основні аспекти забезпечення ефективності функціонування системи протидії легалізації доходів, отриманих у сфері кіберзлочинності, у країнах Європейського Союзу узагальнимо на рис. 3.2.

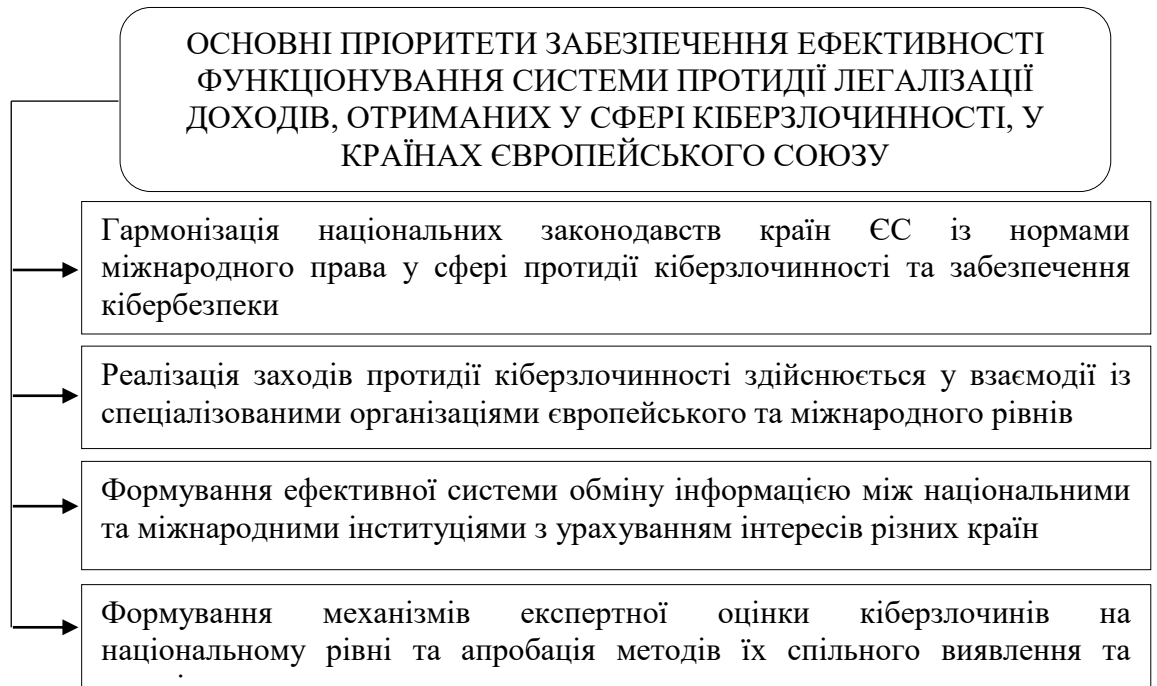


Рис. 3.2. Пріоритетні напрями забезпечення ефективності функціонування системи протидії легалізації доходів, отриманих у сфері кіберзлочинності, у країнах Європейського Союзу

Джерело: власна авторська розробка

При цьому, зазначимо, що на рівні Європейського Союзу започатковано діяльність спеціальних комп'ютерних груп, що здійснюють реагування на випадки прояву кіберзагроз у віртуальному середовищі. Такі групи іменуються як CERT та, в основному, спрямовують свою діяльність на систематизацію даних про кіберпрецеденти та надзвичайні ситуації, які виникають у кіберсередовищі, а також займаються реєстрацією кіберзлочинів й надають допомогу постраждалим з метою мінімізації впливу кібератак.

Не менш вагомою є діяльність міжнародних організацій у сфері попередження та протидії кіберзлочинності, а саме:

- 1) Комп'ютерної групи швидкого реагування, яка створює спеціальні технологічні датчики, що допомагають виявляти кібератаки та отримувати інформацію про потенційні спроби вчинення кіберзлочинів;
- 2) Європейського центру боротьби з кіберзлочинністю, з яким співпрацює Комп'ютерна група швидкого реагування та передає інформацію

про спроби вчинення кіберзлочинів, де вона узагальнюється та опрацьовується;

3) Європейської агенції оборони, до компетенції якої входить виявлення підстав для проведення спеціальних кібероперацій;

4) Європейської агенції з питань мережевої та інформаційної безпеки, що формує й реалізовує механізми виявлення та блокування кібератак чим попереджує вчинення кіберзлочинів.

Очевидно, що досягнення позитивних результатів стає можливим лише при умові комплексної взаємодії та реалізації цілого спектру визначених заходів. Проте, варто констатувати, що Україні необхідно посилити процеси налагодження міжнародної взаємодії у сфері протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Отже, результати вивчення міжнародного досвіду удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності, свідчать про те, що високо розвинуті країни спроможні забезпечити вищі стандарти антилегалізаційної боротьби, ніж країни із низьким рівнем соціально-економічного розвитку. Доведено необхідність посилення міждержавної взаємодії України із зарубіжними країнами та міжнародними організаціями, що займаються питаннями протидії кіберзлочинності та легалізації коштів, одержаних внаслідок вчинення кіберзлочинів.

Висновки до розділу 3

1. Результати проведених досліджень щодо визначення оптимальних напрямів удосконалення заходів протидії легалізації доходів, отриманих у сфері кіберзлочинності дозволяють окреслити основні стратегічні пріоритети протидії кіберзлочинності. Встановлено, що в найближчій перспективі необхідним виявляється удосконалення нормативно-правового й законодавчого забезпечення діяльності у таких сферах як кібербезпека, кіберзахист та кіберохорона; інтенсифікація й стимулювання інноваційного розвитку технологічної складової національної системи кібербезпеки; забезпечення ефективної міжнародної взаємодії та співробітництва із зарубіжними партнерами; удосконалення організаційної та технічної моделей розвитку системи кіберзахисту; розширення напрямків проведення наукових досліджень з питань забезпечення кібероборони та кіберзахисту; розроблення ефективних механізмів кіберзахисту об'єктів, що належать до критичної інформаційної інфраструктури та формування програм підготовки фахівців у сфері кібербезпеки.

2. Виявлено необхідність розроблення та прийняття Закону України «Про державно-приватне партнерство у сфері кібербезпеки», а також розроблення системи проведення аудиту інформаційної безпеки і методики його проведення. Обґрунтовано відсутність методичного інструментарію проведення статистичних досліджень стану та динаміки зміни кіберзлочинності в Україні, що потребує законодавчого врегулювання даної проблеми. Доведено потребу у посиленні основних аспектів підвищення кіберграмотності населення, що можна досягнути шляхом розроблення та реалізації Загальнодержавної програми кіберграмотності населення.

3. Узагальнення міжнародного досвіду удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності, дозволяє стверджувати, що найбільш оптимальною системою протидії легалізації

доходів, отриманих у сфері кіберзлочинності є система, що запроваджена у США. Обґрунтовано необхідність адаптації позитивних європейських практик протидії кіберзлочинності до умов функціонування України. Встановлено необхідність посилення взаємодії правоохоронних органів України із міжнародними органами у сфері протидії легалізації доходів, отриманих у сфері кіберзлочинності та поширенню кіберзлочинності.

ВИСНОВКИ

У кваліфікаційній роботі проведено обґрунтування теоретичних засад та практичних аспектів забезпечення ефективної протидії легалізації доходів, отриманих у сфері кіберзлочинності, на підставі чого можна здійснити узагальнення наукових підходів щодо визначення сутності легалізаційних процесів та кіберзлочинності, охарактеризувати сучасний стан кіберзлочинності в Україні та оцінити обсяги легалізації доходів, отриманих у сфері кіберзлочинності, окреслити стратегічні пріоритети протидії кіберзлочинності та розглянути можливості адаптації позитивного міжнародного досвіду удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності. Зазначене дає підстави зробити наступні висновки:

1. Проведений компаративний аналіз дозволяє визначити сутність легалізаційних процесів, під якими розуміється злочинна діяльність, що пов'язана із вчиненням діянь, які передбачають приховування джерел походження, місця знаходження та використання грошових коштів, майна та інших нелегальних активів з метою збагачення та одержання неправомірної вигоди. Встановлено, що причинами виникнення та інтенсифікації легалізаційних процесів є значне накопичення нелегально одержаних грошових коштів, майна та інших активів та необхідність їх залучення в офіційний сектор економіки. Виявлено деструктивний вплив легалізаційних процесів на економіку країни та на суспільство.

2. З'ясовано, що кіберзлочинність є складним та небезпечним соціально-економічним явищем, що являє собою сукупність злочинів, які вчиняються за допомогою комп'ютера у віртуальному інформаційному просторі, де систематизовані й зберігаються відомості про процеси, явища та факти, дані про осіб в процесі руху по локальних і глобальних комп'ютерних системах. Окреслено основні види кіберзлочинності, до який відноситься

порушення авторського і суміжних прав; шахрайство та встановлення доступу до банківської й комерційної таємниці; крадіжки персональних даних, особистої й приватної інформації; незаконні дії з документами на переказ; крадіжки коштів з банківських рахунків та платіжних карток; виготовлення, збут та ввезення на територію країни порнографічних матеріалів та ухилення від сплати податків. Виявлено, що основні способи протидії кіберзлочинності передбачають посилення відповідальності за вчинення кіберзлочинів та налагодження міжвідомчої й міжнародної взаємодії у сфері боротьби із економічною злочинністю.

3. Проведений аналіз сучасного стану кіберзлочинності в Україні дає підстави стверджувати про зростання показників кіберзлочинності в нестійких умовах невизначеності та посилення фінансово-економічної й суспільно-політичної криз в Україні. Встановлено зростаючі тенденції щодо поширення кіберзлочинності та виникнення нових схем вчинення кіберзлочинів, які використовуються не лише для накопичення неправомірно одержаних грошових коштів, майна та інших активів, а й для легалізації тіньових капіталів. Виявлено, що найбільшу частку у структурі кіберзлочинів, вчинених в Україні у 2017–2023 рр. складає онлайн шахрайство.

4. Здійснення емпіричних оцінювань обсягів легалізації доходів, отриманих у сфері кіберзлочинності, дозволило встановити, що кіберзлочинність становить значну загрозу інтересам України та спричинює недофінансування Державного бюджету. Доведено зростаючі тенденції щодо обсягів легалізації доходів, отриманих у сфері кіберзлочинності. Виявлено позитивні аспекти щодо взаємодії Державної служби фінансового моніторингу України із правоохоронними органами.

5. Окреслено основні стратегічні пріоритети протидії кіберзлочинності в Україні, серед яких обґрунтованим виявляється необхідність удосконалення чинного законодавства та нормативно-правового забезпечення в частині прийняття Закону України «Про державно-приватне

партнерство у сфері кібербезпеки», розроблення методики проведення аудиту інформаційної безпеки, формування методичного інструментарію проведення статистичних досліджень стану та динаміки зміни кіберзлочинності в Україні, а також розроблення та реалізації Загальнодержавної програми кіберграмотності задля підвищення кіберграмотності населення.

6. Систематизовано міжнародний досвід удосконалення системи протидії легалізації доходів, отриманих у сфері кіберзлочинності, та доведено потребу у посиленні міждержавної взаємодії України із зарубіжними країнами та міжнародними організаціями щодо протидії кіберзлочинності та легалізації коштів, одержаних внаслідок вчинення кіберзлочинів. Обґрунтовано доцільність запозичення світового досвіду боротьби з кіберзлочинністю та необхідність адаптації позитивних європейських практик протидії кіберзлочинності до умов функціонування України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бех О. Протидія легалізації доходів, одержаних злочинним шляхом. *Підприємництво, господарство і право*. 2021. № 2. С. 213–218. URL: DOI <https://doi.org/10.32849/2663-5313/2021.2.38>.
2. Аркуша Л.І. Сутність виявлення легалізації (відмивання) доходів, одержаних злочинним шляхом. *Сучасні проблеми правового, економічного та соціального розвитку держави*. 2017. С. 139–141. URL: https://univd.edu.ua/general/publishing/konf/01_12_2017/pdf/41.pdf.
3. Гончарук В.Л. Вплив легалізації (відмивання) доходів, одержаних злочинним шляхом, на економічну сферу України в сучасних умовах. *Кримінальне право, кримінальний процес та криміналістика*. 2021. № 4. С. 124–130. URL: DOI 10.32782/LAW.UA.2021.4.18.
4. Лугіна Н.А., Омелян М.В. Кримінологічна характеристика легалізації (відмивання) доходів, одержаних злочинним шляхом. *Ірпінський юридичний часопис: науковий журнал*. 2019. Вип. 2. С. 158–165. URL: DOI 10.33244/2617-4154.2.2019.158-165.
5. Чебукіна Д.О. Кримінально-правова характеристика легалізації (відмивання) доходів, одержаних злочинним шляхом. *Науковий журнал «ЛОГОЗ. Мистецтво наукової думки»*. 2019. № 4. С. 185–189.
6. Blikhar M.M., Ortynska N.V., Dufeniuk O.M., Vinichuk M.V., Matviienko O.I. Economic and legal mechanism for combating legalization (laundering) of income resulting from tax evasion in the context of deoffshorization of Ukraine's economy. *Фінансово-кредитна діяльність: проблеми теорії та практики. Збірник наукових праць*. 2021. Випуск 5 (40). 630 с. (с. 497–505). URL: DOI: 10.18371/fcaptp.v5i40.245204.
7. Завидняк І.О. Легалізація (відмивання) коштів, одержаних злочинним шляхом, як один з видів економічних транснаціональних злочинів. *Електронне наукове видання «Аналітично-порівняльне*

правознавство». 2021. С. 313–317. URL: DOI <https://doi.org/10.24144/2788-6018.2021.04.54>.

8. Фролов С. Кримінально-правова та кримінологічна характеристика легалізації (відмивання) доходів, одержаних злочинним шляхом. *Юридичний вісник*. 2019. № 4. С. 130–136. URL: DOI <https://doi.org/10.32837/yuv.v0i4.980>.

9. Уткіна М.С. Міжнародні стандарти та міжнародне співробітництво у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом. *Дніпровський науковий часопис публічного управління, психології, права*. 2023. URL: DOI: [10.51547/ppp.dp.ua/2023.3.29](https://doi.org/10.51547/ppp.dp.ua/2023.3.29).

10. Blikhar M.M., Vinichuk M.V., Komarnytska I.I., Zaiats O.S., Kashchuk M.H. Counteraction to financial crimes in the system of fight against legalization (laundering) of criminally obtained funds. *Financial and Credit Activities: Problems of Theory and Practice*. 2022. Vol. 1 (42). 536 p. (P. 73–83). URL: DOI: <https://doi.org/10.55643/fcaptp.1.42.2022.3704>.

11. Білоус І.І. Сутнісна характеристика легалізації доходів, одержаних злочинним шляхом. *Економіка та держава*. 2019. № 5. С. 82–88. URL: DOI: [10.32702/2306-6806.2019.5.82](https://doi.org/10.32702/2306-6806.2019.5.82).

12. Blikhar M.M., Savchenko L.A., Komarnytska I.I., Vinichuk M.V. Strategic orientaries of legalization of the economy of Ukraine: economic and legal aspects. *Фінансово-кредитна діяльність: проблеми теорії та практики. Збірник наукових праць*. 2019. Випуск 2 (29). 534 с. (С. 101–112). URL: DOI: [http://doi.org/10.18371/fcaptp.v2i29.171850](https://doi.org/10.18371/fcaptp.v2i29.171850).

13. Грабовський Л.А. Протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, як складова забезпечення економічної безпеки України. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2 (10-11). С. 200–205.

14. Діордіца І.В. Поняття та зміст кіберзлочинності. *Глобальна організація союзницького лідерства*. 2017. URL: <https://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/>.
15. Никончук Н.С. Маслова О.О. Кіберзлочинність в Україні: виклики сучасності. *Юридичний науковий електронний журнал*. 2021. № 9. С. 202–205. URL: DOI <https://doi.org/10.32782/2524-0374/2021-9/49>.
16. Таран О.В., Гавловський В.Д. Організована кіберзлочинність в Україні: проблеми формування офіційної статистики та її аналізу. *Інформація і право*. 2021. № 4(39). С. 193–201.
17. Неділько Я.В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60. URL: <http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf>.
18. Неділько Я.В. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». Київ: Київський національний університет ім. Т.Г. Шевченка. 257 с. URL: <https://uacademic.info/ua/document/0823U101422>.
19. Бодунова О.М. Історико-правові аспекти виникнення кіберзлочинності. *Держава та регіони*. 2020. № 3(69). Том 3. С. 143–147. URL: DOI <https://doi.org/10.32840/1813-338X-2020.3.3.24>.
20. Конвенція про кіберзлочинність від 23.11.2001. № 994_575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
21. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163–VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0#w1_1.
22. Кримінального кодексу України від 05.04.2001 р. № 2341–III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.

23. Fischerkeller M.P. Current International Law is Not an Adequate Regime for Cyberspace. *LawFare, International Law*. 2021. URL: <https://www.lawfaremedia.org/article/current-international-law-not-adequate-regime-cyberspace>.

24. Кундеус В.Г. Поняття та види кіберзлочинів. Держава і злочинність. Нові виклики в епоху постмодерну. Харків, 2020. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content>.

25. Звіт Національної поліції України про результати роботи у 2017 р. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/zvitnpu2017textgrafic.pdf.

26. Звіт Національної поліції України про результати роботи у 2018 р. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/Zvit_NPU_2018.pdf.

27. Звіт Національної поліції України про результати роботи у 2019 р. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf.

28. Звіт Національної поліції України про результати роботи у 2020 р. URL: <https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf>.

29. Звіт Національної поліції України про результати роботи у 2021 р. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2021/Zvit_NPU_2021_.pdf.

30. Звіт Національної поліції України про результати роботи у 2022 р. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2022/Zvit_polic_2022.pdf.

31. Звіт Національної поліції України про результати роботи у 2023 р. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/zvit_NPU_2023.pdf.

32. Global Cybersecurity Index 2017. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.
33. Global Cybersecurity Index 2018. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
34. Global Cybersecurity Index 2019. URL: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/>.
35. Global Cybersecurity Index 2020. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
36. Global Cybersecurity Index 2021. URL: <https://www.itu.int/pub/D-STR-GCI.01-2021>.
37. Global Cybersecurity Index 2022. URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.
38. Global Cybersecurity Index 2023. URL: <https://seon.io/resources/global-cybercrime-report>.
39. Звіт Державної служби фінансового моніторингу України за 2017 рік. URL: https://fiu.gov.ua/assets/userfiles/0350/zvity/zvit_2017_UA.pdf.
40. Звіт Державної служби фінансового моніторингу України за 2018 рік. URL: https://fiu.gov.ua/assets/userfiles/0350/zvity/zvit_2018_ukr.pdf.
41. Звіт Державної служби фінансового моніторингу України за 2019 рік. URL: <https://fiu.gov.ua/assets/userfiles/0350/zvity/zvit2019ua.pdf>.
42. Звіт Державної служби фінансового моніторингу України за 2020 рік. URL: <https://fiu.gov.ua/assets/userfiles/0350/zvity/PublicZvit2020.pdf>.
43. Звіт Державної служби фінансового моніторингу України за 2021 рік. URL: <https://fiu.gov.ua/assets/userfiles/0350/zvity/zvit2021ukr.pdf>.
44. Звіт Державної служби фінансового моніторингу України за 2022 рік. URL: <https://fiu.gov.ua/assets/userfiles/0350/zvity/zvit2022ukr.pdf>.
45. Звіт Державної служби фінансового моніторингу України за 2023 рік. URL: <https://fiu.gov.ua/assets/userfiles/0350/zvity/zvit2023ukr.pdf>.

46. Про Стратегію кібербезпеки України: рішення Ради національної безпеки і оборони України від 14.05.2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/n0055525-21#Text>.

47. Про затвердження Плану заходів на 2023–2024 рр. з реалізації Стратегії кібербезпеки України: розпорядження Кабінету міністрів України від 19.12.2023 р. № 1163-р. URL: <https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text>.

48. Сербин Р.А. Окремі засади взаємодії між Державною службою фінансового моніторингу України, суб'єктами державного моніторингу, правоохоронними, судовими та міжнародними органами під час запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом. *Юридичний науковий електронний журнал*. 2023. № 1. С. 626–628. URL: DOI <https://doi.org/10.32782/2524-0374/2023-1/147>.

49. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels. 07.03.2013. URL: <https://www.enisa.europa.eu/>.