МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ІНСТИТУТ УПРАВЛІННЯ, ПСИХОЛОГІЇ ТА БЕЗПЕКИ

Кафедра фінансів та обліку

ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

кваліфікаційна робота
здобувача вищої освіт
2 курсу денної форми навчання
МЕЛЬНИКА Андрія Миколайовича

Науковий керівник
доктор економічних наук, доцент
МЕЛЬНИК Степан Іванович

Рецензент
доктор економічних наук, професор
ШТАНГРЕТ Андрій Михайлович

Кваліфікаційна робота допущена до захисту
«05» грудня 2022 р., протокол № 7
завідувач кафедри фінансів та обліку

_____ МЕЛЬНИК С.І.
(підпис) (ПРІЗВИЩЕ та ініціали)

Львів
2022

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Інститут *управління, психології та безпеки*
Кафедра *фінансів та обліку*
Освітній ступінь «*магістр»*
Галузь знань *07 «Управління та адміністрування»*
Спеціальність *072 «Фінанси, банківська справа та страхування»*
Назва освітньої програми «*Фінансова розвідка»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
фінансів та обліку
_____Степан МЕЛЬНИК
«01» липня 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
МЕЛЬНИКА Андрія Миколайовича

1. Тема роботи **«Протидія легалізації доходів, отриманих у сфері кіберзлочинності»**
керівник роботи **МЕЛЬНИК Степан Іванович, доктор економічних наук, доцент**
затверджені наказом ЛьвДУВС від **«30» червня 2022 р. № 638 о/с**
2. Термін подання здобувачем вищої освіти роботи **«05» грудня 2022 р.**
3. Вихідні дані до роботи Законодавчі та нормативно-правові документи з питань протидії легалізації доходів, отриманих у сфері кіберзлочинності, літературні джерела із зазначеної тематики, статистичні та аналітичні дані.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Провести теоретичне дослідження сутності та значення легалізації доходів, отриманих злочинним шляхом та кіберзлочинності, її видів, наслідків та способів протидії; проаналізувати обсяги легалізації доходів, отриманих у сфері кіберзлочинності, в Україні; здійснити оцінку динаміки кіберзлочинності в Україні; запропонувати напрями удосконалення національної системи протидії кіберзлочинності; узагальнити досвід зарубіжних країн щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності.
5. Перелік графічного матеріалу (додатків). Схеми легалізації доходів, отриманих злочинним шляхом, основні стадії легалізації доходів, отриманих злочинним шляхом, основні причини виникнення та розвитку кіберзлочинності, основні види кіберзлочинів, схема здійснення кіберзлочинів із використання шахрайства щодо заволодіння коштами підприємств-нерезидентів, схема здійснення кіберзлочинів через несанкціоноване заволодіння активами шляхом несанкціонованого списання коштів підприємств-нерезидентів, схема здійснення кіберзлочинів шляхом незаконного списання грошових коштів з банківських рахунків через дистанційне керування, динаміка обсягів легалізованих (відмитих) коштів, що були отримані внаслідок злочинних діянь в Україні у 2017–2021 рр., динаміка кількості матеріалів, сформованих Держфінмоніторингом та переданих до правоохоронних та розвідувальних органів у 2017–2021 рр., динаміка загальної кількості виявлених в Україні кіберзлочинів у 2017–2021 рр., динаміка кількості виявлених в Україні кіберзлочинів відповідно до сфери діяльності у 2017–2021 рр., динаміка Глобального індексу кібербезпеки в Україні у 2017–2021 рр., динаміка Глобального індексу кібербезпеки в країнах Європейського Союзу та в інших країнах світу у 2017–2021 рр., групування країн світу за показником Глобального індексу кібербезпеки у 2017–2021 рр., динаміка сумарних витрат на кібербезпеку в країнах світу у 2017–2021 рр., система забезпечення кібербезпеки держави, основні напрямки протидії кіберзлочинності в Україні, основні стратегічні

пріоритети забезпечення кіберзахисту та зміцнення кібербезпеки в Україні, основні шляхи запозичення позитивного міжнародного досвіду протидії кіберзлочинності.

6. Консультанти розділів роботи

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	МЕЛЬНИК С. І.		
2	МЕЛЬНИК С. І.		
3	МЕЛЬНИК С. І.		

7. Дата видачі завдання «01» липня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Опрацювання літератури за темою роботи та складання плану	01.08.2022	виконано
2	Написання першого розділу	01.09.2022	виконано
3	Написання другого розділу	01.10.2022	виконано
4	Написання третього розділу	01.11.2022	виконано
5	Підведення підсумків та формулювання висновків	15.11.2022	виконано
6	Оформлення роботи	01.12.2022	виконано

Здобувач вищої освіти _____ МЕЛЬНИК А. М.
(підпис) (ПРІЗВИЩЕ та ініціали)

Науковий керівник _____ МЕЛЬНИК С. І.
(підпис) (ПРІЗВИЩЕ та ініціали)

АНОТАЦІЯ

МЕЛЬНИК А.М. Протидія легалізації доходів, отриманих у сфері кіберзлочинності. – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 072 «Фінанси, банківська справа та страхування». – Львівський державний університет внутрішніх справ МВС України, Львів, 2022.

Кваліфікаційна робота присвячена дослідженню теоретико-прикладних засад протидії легалізації доходів, отриманих у сфері кіберзлочинності. Розглянуто теоретичні аспекти протидії легалізації доходів, отриманих у сфері кіберзлочинності, визначено сутність кіберзлочинності, її види, наслідки поширення та способи протидії. Проаналізовано стан та тенденції протидії легалізації доходів, отриманих у сфері кіберзлочинності, оцінено динаміку кіберзлочинності в Україні. Визначено стратегічні пріоритети протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Ключові слова: протидія легалізації доходів, кіберпростір, кіберзлочинність, кібербезпека, віртуальний простір, комп’ютерні системи, кіберзлочини.

ANNOTATION

MELNYK A.M. Anti-laundering of proceeds received in the field of cybercrime. – Manuscript.

Qualification work for the master's degree in the specialty 072 "Finance, banking and insurance". – Lviv State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Lviv, 2022.

Qualification work is devoted to the study of the theoretical foundations of combating the legalization of income obtained in the field of cybercrime. The theoretical principles of combating the legalization of income obtained in the field of cybercrime are considered, the essence of cybercrime, its types, consequences and methods of countermeasures are determined. The state and trends of combating the legalization of income obtained in the field of cybercrime were analyzed, and the dynamics of cybercrime in Ukraine were assessed. The strategic priorities of combating the legalization of income obtained in the field of cybercrime have been determined.

Key words: combating money laundering, cyberspace, cybercrime, cyber security, virtual space, computer systems, cybercrimes.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Інтенсифікація розвитку цифрових технологій та їх поширеність на систему фінансово-економічних відносин активізувала розвиток кіберзлочинності, яка становить значну загрозу національній та міжнародній економічній системі. Здійснення фінансових операцій у кіберпросторі стимулює розвиток фінансових інновацій та, водночас, зумовлює вчинення протиправних діянь, що обумовлено прагненням сформувати тіньові капітали та легалізувати доходи, отримані у сфері кіберзлочинності.

Проблемі аспекти дослідження протидії легалізації доходів, отриманих у сфері кіберзлочинності, перебувають в центрі уваги таких науковців як Р. Баранов, І. Білоус, О. Глущенко, О. Дудоров, С. Лєонов, О. Підхомний, О. Рєзнік, М. Флейчук, О. Халін, напрацювання яких використано у кваліфікаційній роботі. Водночас, при написанні кваліфікаційної роботи широко використовувалися закони України, аналітичні дані Державної служби фінансового моніторингу України, Національної поліції України та міжнародних організацій, що здійснюють діяльність у сфері протидії кіберзлочинності, інформаційні ресурси, доступні через мережу Інтернет. Проте, не заперечуючи вагомого наукового доробку щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності, досягнути бажаного результату досі не вдалося, що потребує поглиблення досліджень у даному керунку, а тематика набуває особливої актуальності.

Мета і завдання дослідження. Метою кваліфікаційної роботи є обґрунтування теоретико-методичних засад протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Досягнення поставленої мети потребує вирішення таких основних **завдань**:

– визначити сутність та з’ясувати значення легалізації доходів, отриманих злочинним шляхом;

– дослідити кіберзлочинність, виявити її види, наслідки та способи протидії;

– проаналізувати обсяги легалізації доходів, отриманих у сфері кіберзлочинності, в Україні;

– здійснити оцінку динаміки кіберзлочинності в Україні;

– запропонувати напрями удосконалення національної системи протидії кіберзлочинності;

– узагальнити досвід зарубіжних країн щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності.

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

Предметом дослідження є теоретико-прикладні засади дослідження стану та тенденцій протидії легалізації доходів, отриманих у сфері кіберзлочинності.

Методи дослідження. У кваліфікаційній роботі використано методи економічного аналізу та інших фундаментальних досліджень. Визначення сутності наукових категорій «легалізація доходів, отриманих злочинним шляхом» та «кіберзлочинність» здійснено за допомогою методу спостереження та системного аналізу. Аналіз обсягів легалізації доходів, отриманих злочинним шляхом, та оцінювання стану й тенденцій розвитку кіберзлочинності проведено із використанням методу статистичного аналізу, порівняння та функціонально-системного підходу. Дослідження напрямів удосконалення національної системи протидії кіберзлочинності здійснено за допомогою методу синтезу та компаративного аналізу. Метод узагальнення та систематизації застосовано при формуванні висновків за результатами проведеного дослідження.

Наукова новизна одержаних результатів:

– удосконалено основні напрями протидії кіберзлочинності в Україні шляхом пропозиції формування ефективної системи кібербезпеки

держави; удосконалення чинного законодавства в частині регулювання відносин у кіберпросторі та посилення взаємної міжнародної співпраці.

Основний зміст роботи. У першому розділі кваліфікаційної роботи розкрито сутність легалізації доходів, отриманих злочинним шляхом, та встановлено її значення для економіки й суспільства, окреслено основні види кіберзлочинності та способи протидії даному негативному явищу. У другому розділі проаналізовано обсяги легалізації доходів, отриманих злочинним шляхом, у кіберпросторі та оцінено динаміку кіберзлочинності в Україні. У третьому розділі досліджено досвід зарубіжних країн щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності та визначено основні стратегічні пріоритети протидії кіберзлочинності в Україні.

Структура роботи. Кваліфікаційна робота складається із анотації українською та англійською мовами, вступу, трьох розділів, висновків та списку використаних джерел (52 найменування на 6 сторінках). Загальний обсяг роботи становить 61 сторінка, з них основний текст – 51 сторінка, які містять 18 рисунків та 1 таблицю.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

1.1. Сутність та значення легалізації доходів, отриманих злочинним шляхом

Зростаючі масштаби тінізації економіки зумовлюють накопичення значних обсягів капіталів, які сформовані поза офіційним сектором економіки та потребують узаконення й набуття легального вигляду, що стимулює розвиток такого явища як легалізація доходів, отриманих злочинним шляхом. Сучасні тенденції функціонування національної економіки засвідчують поглиблення значних деструктивних змін економіки й суспільства та вимагають розроблення комплексних заходів протидії негативним чинникам, адже обсяги легалізованих капіталів досягнули критичного рівня та загрожують стабільності глобальної фінансової системи.

Проблематика дослідження легалізації доходів, отриманих злочинним шляхом, набуває особливої значущості в умовах сьогодення, оскільки впродовж останніх років інтенсифікується розвиток економічної злочинності, суспільна небезпека якої посилюється швидкими темпами розвитку віртуального середовища здійснення господарської діяльності та активізацією злочинної діяльності у кіберпросторі. Поява нових фінансових технологій та транснаціональний характер організованої злочинності в економіці потребує зваженого підходу до вирішення проблем запобігання даному деструктивному явищу та з’ясування його особливостей.

Легалізація доходів, отриманих злочинним шляхом, у розумінні М Флейчук [1, с. 515] пов’язана із диспропорціями соціально-економічного розвитку країни та потребою недобросовісних суб’єктів господарювання у виведенні із тіньового сектору економіки протизаконних капіталів.

І. Білоус [2, с. 85] переконана, що легалізація доходів, отриманих злочинним шляхом, трактується як процес перетворення протиправно одержаних активів в легальний капітал шляхом приховування дійсного джерела походження таких активів та фактів здійснення злочинних операцій у фінансовій сфері.

Натомість О. Дудоров та Т. Тертиченко [3, с. 9] появу явища легалізації доходів обумовлюють посиленням глобалізаційних та інтеграційних процесів, а також злиттям національних фінансових ринків й утворенням інтегрованої міжнародної фінансово-економічної системи. Сам процес легалізації тіньових капіталів науковці асоціюють із вчиненням зумисних дій, які направлені на узаконення протиправних активів та надання їм статусу легально одержаних [3, с. 33].

В даному контексті, Р. Баранов [4, с. 65] стверджує, що легалізація доходів, отриманих злочинним шляхом, набуває глобального характеру через постійне оновлення схем здійснення даного протиправного діяння та тісну взаємодію із організованою злочинністю. Науковець відмічає високий рівень участі у легалізації протиправних капіталів комерційних банків та фінансових установ, а також дослідив активізацію легалізаційних процесів із застосуванням електронних грошей.

О. Рєзнік та Н. Щербак [5, с. 291–292] процес легалізації доходів, отриманих злочинним шляхом, характеризують як проведення через фінансову систему держави нелегально одержаних коштів з метою надання їм вигляду законних активів, приховування джерела походження та власника. В процесі здійснених досліджень науковці дійшли висновку, що основні схеми легалізації доходів, отриманих злочинним шляхом, варто виокремлювати в залежності від джерела їх походження, каналів реалізації легалізаційних схем, видів активів та інституцій, що беруть участь у такого роду протиправних діяннях. Систематизацію зазначеного відобразимо на рис. 1.1.

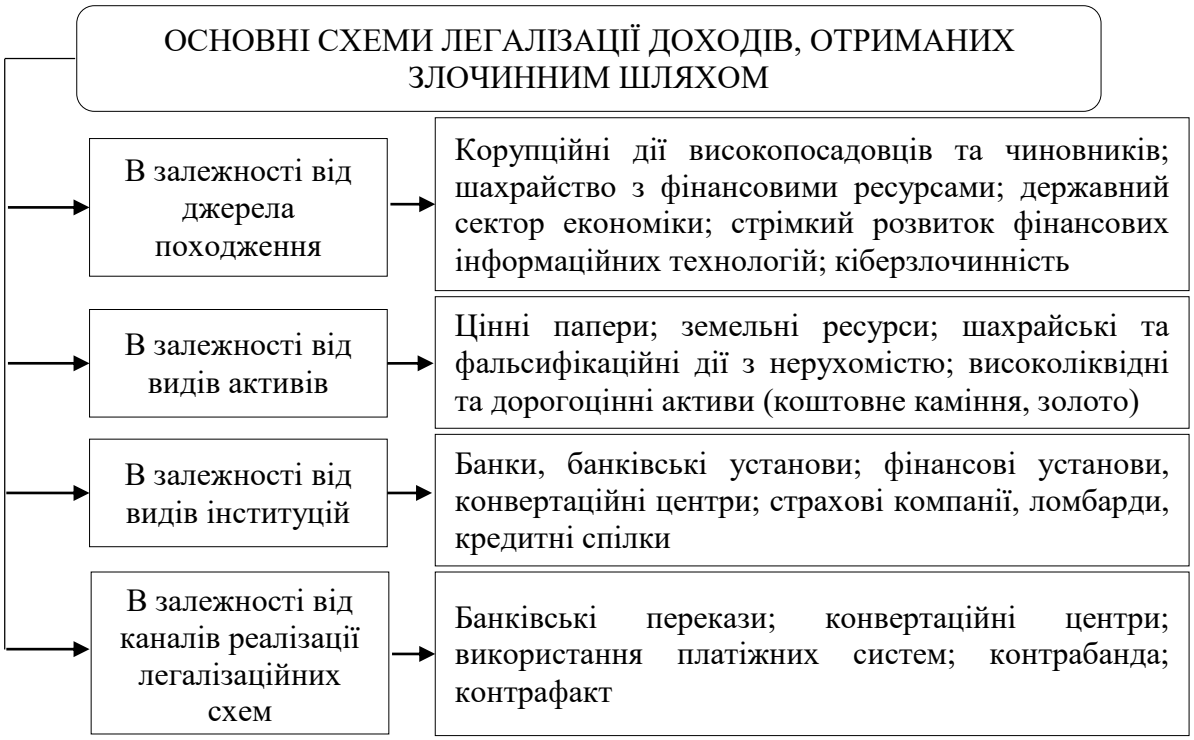


Рис. 1.1. Основні схеми легалізації доходів, отриманих злочинним шляхом

Джерело: складено автором за даними [4, с. 292]

С. Лєонов, А. Бойко та С. Миненко [6, с. 36] легалізацію кримінальних доходів розглядають як вчинення зумисних дій фінансового характеру, що призводить до приховування й маскування первинного джерела походження фінансових активів та інших правочинів, що з ними пов'язані або володіння такими ресурсами.

І. Гончаренко [7, с. 246] легалізацію доходів, отриманих злочинним шляхом, вважає значною проблемою реалізації державної політики та забезпечення сталого соціально-економічного розвитку країни, а також першоджерелом інтенсифікації економічної злочинності в країні. Очевидно, що розвиток цифрових технологій та поступова діджиталізація економіки зміщують вектор вчинення протиправних діянь із фінансовими ресурсами в напрямку віртуального середовища, широко використовуючи суб’єкти фінансово-банківського сектору, що порушує проблему кіберзахисту національної фінансово-економічної системи.

Ю. Тарнавський, Д. Беседа, Т. Момотенко, О. Суворов та О. Каракасіді [8] вагомого значення надають тому факту, що легалізацію доходів, отриманих злочинним шляхом, відповідно до класифікації ООН, віднесено до ключових складових транснаціональної економічної злочинності, яка загрожує не лише зниженням рівня соціально-економічного розвитку держави, а й створює значні диспропорції в економічній сфері та суспільстві.

При цьому, Л. Дубіняк [9] стверджує, що легалізація результатів злочинної діяльності поступово трансформується у професійну діяльність організованих злочинних угрупувань та перетворюється на свого роду фінансові махінації із нелегальними ресурсами, а О. Халін [10, с. 5] довів її невід'ємність із функціонуванням офшорних зон та вчиненням протиправних діянь в податковій сфері.

Погоджуючись із позицією науковців, С. Фролов [11, с. 130] акцентує увагу на наслідках та суспільних небезпеках легалізації неправомірних доходів, адже вона спричинює значну шкоду офіційному сектору економіки, посилює економічну злочинність та істотно дестабілізує фінансову систему держави. Як наслідок, в країні починають інтенсивно розвиватися інфляційні чинники, недобросовісна конкуренція, диференціація доходів населення та знижується рівень макроекономічної стабільності. Зважаючи на окреслене, дане злочинне діяння С. Фролов називає типовим конвенційним злочином, криміналізація якого обумовлена інтеграційними процесами країни.

Поглиблюючи наукові дослідження в окресленому напрямку, І. Завидняк [12, с. 313] встановив, що по відношенню до економічної злочинності й організованої злочинної діяльності легалізація доходів, отриманих злочинним шляхом, є предикатним злочином, який спрямований на особисте збагачення та одержання неправомірних прибутків. Водночас, науковцем виділено певні стадії легалізації доходів, отриманих у неправомірний спосіб, які відобразимо на рис. 1.2.

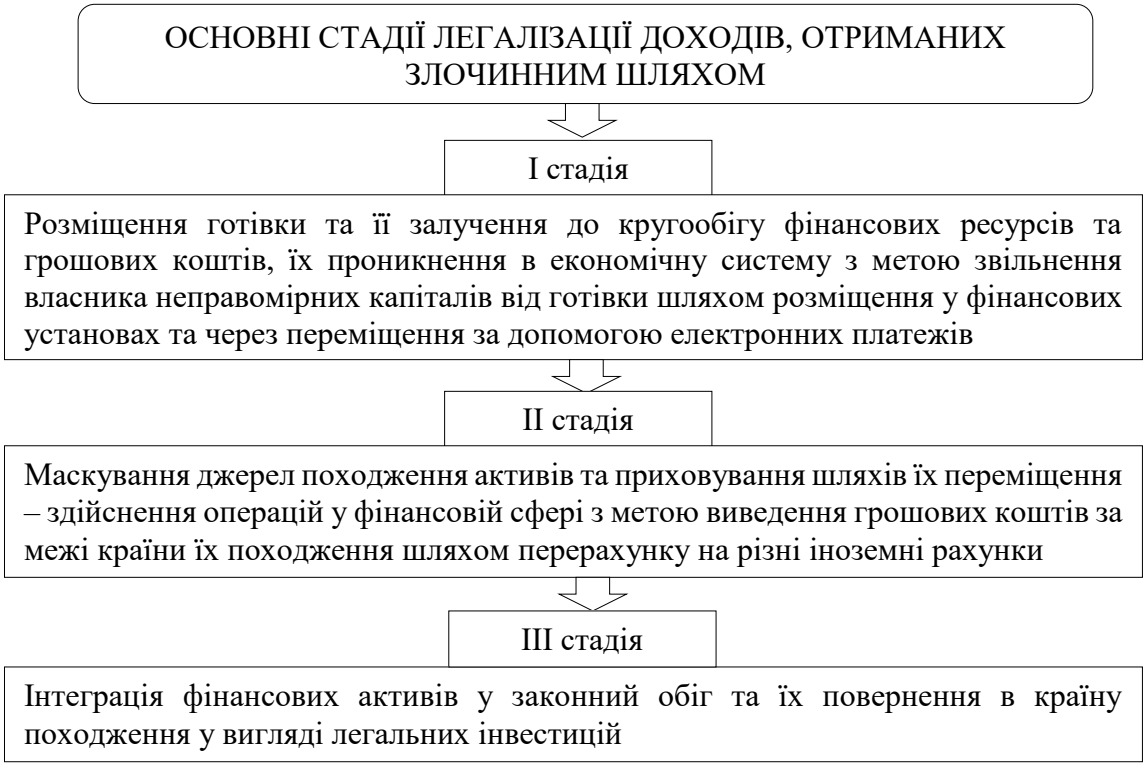


Рис. 1.2. Основні стадії легалізації доходів, отриманих злочинним шляхом

Джерело: складено автором за даними [12, с. 315–316]

Достатньо вагомими можна вважати напрацювання О. Підхомного та О. Глущенка [13, с. 369], які переконують, що на національному рівні необхідно сформувати ефективну систему запобігання та протидії легалізації доходів, одержаних злочинним шляхом, спроможну вчасно виявити причини виникнення даного деструктивного явища та розробити заходи щодо оцінювання основних чинників легалізаційної діяльності у тіньовому секторі економіки, серед яких варто виділити політико-економічні, соціально-правові та морально-психологічні. Крім зазначеної позиції, в науковій думці присутні твердження, що чинники легалізації результатів незаконної економічної діяльності потрібно поділяти на універсальні, які притаманні фінансово-економічним системам країн різних типів розвитку; додаткові, що характерні для країн транзитивного типу та окремо М. Флейчук [1, с. 221] пропонує виділяти чинники, які виникають в економіці України.

Така класифікація чинників розвитку легалізаційних процесів змінює підходи до визначення способів здійснення легалізаційної діяльності, особливості яких, на думку Л. Гули [14, с. 336] полягають у формуванні системи методів, що використовуються з метою залучення нелегальних активів в офіційний сектор економіки.

Зважаючи на загрозливі тенденції поширення легалізаційних процесів виникає необхідність протидії даному деструктивному явищу. Причому, О. Лиман та М. Мозгова [15, с. 59] наполягають на розроблені таких заходів протидії легалізаційним проявам в контексті боротьби з організованою транснаціональною злочинністю.

Цікавими виявляються погляди на легалізацію доходів, отриманих злочинним шляхом, що запропоновані Г. Крайник та В. Заточною [16, с. 141], які полягають у тлумаченні даної економіко-правової категорії з точки зору технологій незаконного збагачення та одержання неправомірної вигоди, які передбачають вчинення логічних та взаємопов’язаних злочинних діянь, останньою ланкою яких і є легалізація. Причому, зафіксовано значний рівень стимулювання такої діяльності за рахунок створення сприятливих умов для господарювання поза офіційним сектором економіки та через відсутність жорстких видів кримінальної відповідальності за вчинення таких діянь.

Водночас, С. Лєонов, А. Бойко, В. Боженко та І. Лучко [17, с. 137] виявили взаємозв’язок між обсягами легалізації кримінальних доходів та рівнем соціально-економічного розвитку країни. З точки зору вчених, вищі темпи зростання злочинності у фінансовій сфері спостерігаються в країнах із низьким рівнем розвитку та в країнах транзитивного типу, оскільки існуюча правова система таких країн не спроможна захистити населення та забезпечити високі значення фінансової безпеки держави.

В останні роки достатньо швидкими темпами розвивається віртуальне середовище функціонування фінансової системи, що обумовлено такими викликами сучасності як запровадження карантинних заходів та повномасштабним вторгненням Росії на територію України, внаслідок чого

виникла необхідність обмежити доступ до готівкових розрахунків. Стає очевидним, що проведення безготівкових розрахунків спричинило інтенсифікацію використання електронних платіжних систем. Своєю чергою, під впливом таких значних деструктивних чинників почала стрімко поширюватися кіберзлочинність, вагомого значення дослідженню якої надає Державна служба фінансового моніторингу України, що здійснює формування типологій легалізації доходів, отриманих злочинним шляхом.

Вважаємо за доцільне відмітити такі типологічні дослідження, які здійснюються Держфінмоніторингом в наступних напрямках:

1) легалізація доходів від корупції;
2) легалізація доходів з використанням страхового ринку;
3) легалізація доходів при здійсненні експортно-імпортних операцій;
4) легалізація доходів на фондовому ринку;
5) легалізація доходів з використанням фіктивного підприємництва та конвертаційних центрів;
6) розкрадання бюджетних коштів та коштів банківських установ;
7) легалізація доходів від кіберзлочинів.

Варто зазначити, що окреслена проблематика різносторонньо досліджується й обговорюється як в науковому середовищі, так і серед практиків. Певні напрацювання щодо зниження обсягів легалізації доходів, отриманих злочинним шляхом, вже існують, однак подолати дане деструктивне явище досі не вдалося.

Таким чином, дослідження теоретичних основ легалізації доходів, отриманих злочинним шляхом, дозволяє визнати, що дане негативне економічне явище присутнє у національній економіці та створює значні її деструктивні зміни, впливає на показники соціально-економічного розвитку країни, дестабілізує ситуацію в суспільстві, створюючи соціальну нерівність населення та інші вагомі проблеми.

1.2. Кіберзлочинність: види, наслідки та способи протидії

Загострення проблем забезпечення стабільності міжнародної та національних економічних систем в умовах системної появи нових викликів і небезпек, обумовлене інтенсифікацією розвитку інформаційних технологій, широким застосування комп'ютерних систем та баз даних у фінансово-економічній сфері країн, створенням додаткових можливостей для вчинення протиправних діянь з фінансовими ресурсами в інформаційному середовищі. За таких умов спостерігається активізація неправомірної діяльності в кіберпросторі, який А. Аль-Махрукі, К. Сіанаін та Т. Кечаді [18, с. 279] розглядають як спеціально створену мережу електронних каналів зв'язку, що злагоджено взаємодіють між собою та функціонують на міжнародному рівні із максимальним забезпеченням конфіденційності та різностороннім захистом баз даних, а саму діяльність, яка порушує усталені норми та процес забезпечення захисту інтересів економічних агентів, трактують як кіберзлочинність.

Проблематика дослідження кіберзлочинності в сучасних умовах є надзвичайно важливою, оскільки виникає нагальна необхідність захисту державних та бізнесових інституцій від зловмисного несанкціонованого стороннього втручання, адже відкритий доступ до глобальних мереж спонукає до незаконних посягань на активи із використанням цифрових технологій, що в сукупності призводить до розвитку кіберзлочинності. Тому, Г. Валорі [19] пропонує значну увагу приділяти захисту персональних даних та постійно удосконалювати розвиток інноваційних технологій в напрямку створення нового програмного забезпечення.

Злочини у віртуальному просторі спрямовані на одержання доступу до персональних даних та банківських рахунків суб'єктів економічних відносин як на національному, так і на глобальному рівні. Зважаючи на значні деструктивні зміни світового господарського порядку, зростання кіберзлочинності постійно інтенсифікується та набуває загрозливих

тенденцій. При цьому, як зазначають Н. Никончук та О. Маслова [20, с. 203–204], кіберзлочинність широко використовується для вчинення інших злочинів, що спостерігаються у фінансовій сфері держави, зокрема, легалізації доходів, отриманих злочинним шляхом, та стверджують, що зростання її обсягів деякою мірою обумовлене низьким рівнем кіберграмотності основної маси населення.

В. Гавловський [21, с. 108] кіберзлочинність ототожнює із вчиненням протиправних діянь з використанням комп'ютерних та телекомунікаційних мереж в кіберпросторі, а причини появи кіберзлочинності пропонує поділяти на економічні, політичні, соціальні та організаційні. Водночас, науковець зауважує, що офіційна статистика досі не відображає детальних відомостей про кіберзлочини, що обумовлює фрагментарний характер заходів щодо їх протидії та створює значні труднощі при виявленні. Більше того, встановлені обсяги втрат від кіберзлочинності в світовому масштабі оцінюються Atlas VPN [22] у розмірі 1 трлн. дол. США у 2020 р. та 6 трлн. дол. США у 2021 р.

О. Таран та В. Гавловський [23, с. 195] кіберзлочинність визначають як сукупність суспільно небезпечних діянь у кіберпросторі, які суперечать принципам його використання та наголошують, що вітчизняним законодавством чітко не визначено категоріального апарату щодо кіберзлочинів та існують дискусійні питання у сфері їх класифікації, а відсутність статистики даних про кіберзлочинність, її структуру та стан криміногенної ситуації у кіберпросторі утруднюють процес формування організаційно-правових заходів ефективної протидії.

Достатньо чітке визначення кіберзлочинності запропонував Я. Неділько [24, с. 54], який стверджує, що кіберзлочинність – це діяльність зловмисників, що посягає на суспільні відносини у різних сферах життєдіяльності людини шляхом використання ресурсів кіберпростору.

В умовах сучасності виділяється значна кількість причин виникнення та розвитку кіберзлочиннності, серед найпоширеніших із яких варто назвати ті,

що систематизовані О. Бондаренком та Д. Рєпіним [25, с. 247], які вважаємо за доцільне відобразити на рис. 1.3.

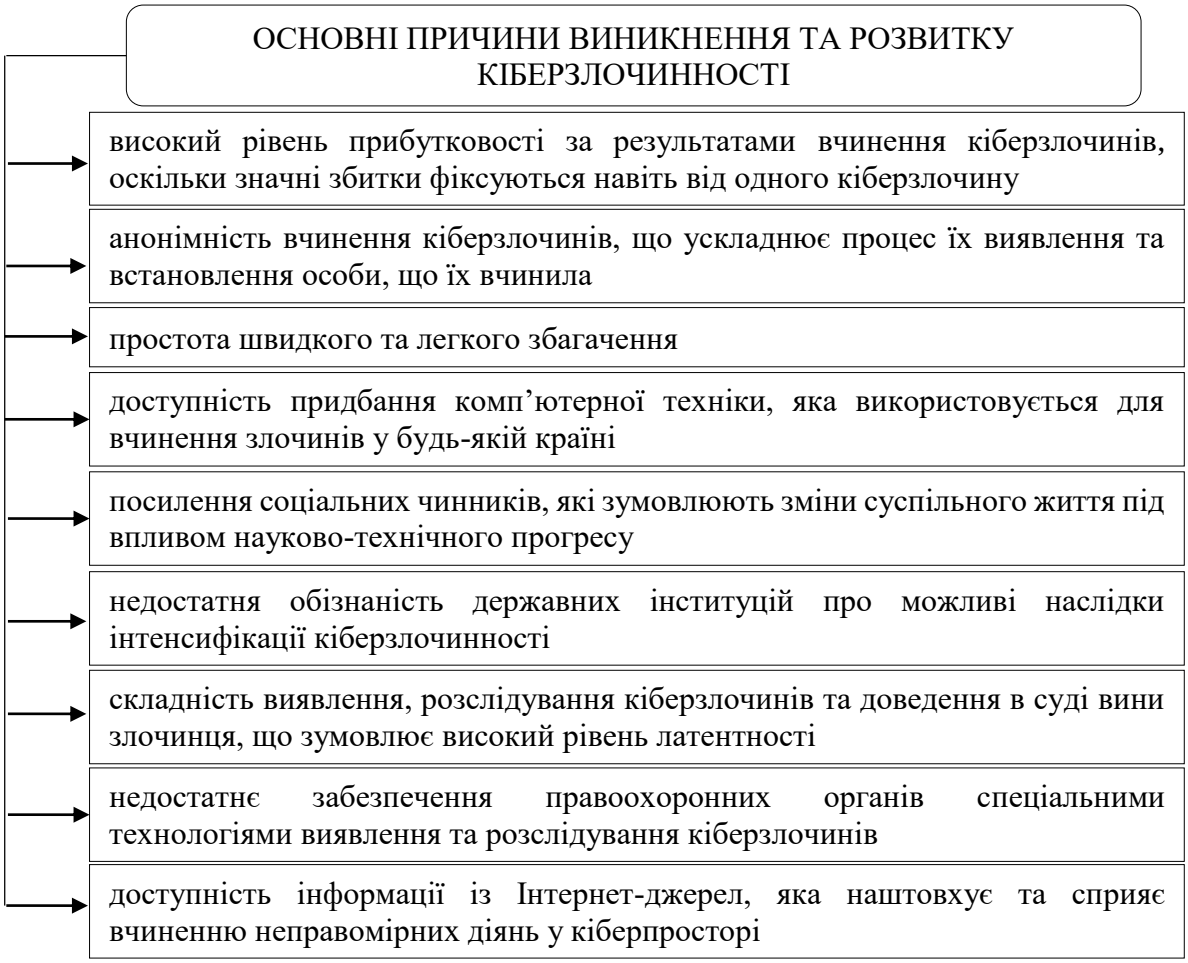


Рис. 1.3. Основні причини виникнення та розвитку кіберзлочинності

Джерело: складено автором за даними [25, с. 247]

Очевидно, що основними причинами стрімкого розвитку кіберзлочинності є прагнення осіб, які вчиняють такі злочини, збагатитися та одержати неправомірну вигоду. Не менш важливим фактором являється відкритість системи доступу до інтернет-ресурсів та технічних засобів, за допомогою яких вчиняються кіберзлочини. Крім того, через відсутність у правоохоронних органів спеціальних засобів для виявлення та розслідування кіберзлочинів їх інтенсифікація постійно зростає, що становить значну загрозу

особливо в сучасних умовах розвитку й переформатування світогосподарського порядку.

М. Фішеркеллер [26] таку ситуацію пов’язує із активізацією процесу створення нових видів кіберзлочинів та їх апробацією на міжнародному рівні, внаслідок чого окремі країни в односторонньому порядку застосовують спеціальні коди з метою нанесення кібервразливостей іншим країнам.

При цьому варто відмітити позитивні напрацювання науковців у напрямку виокремлення найпоширеніших видів кіберзлочиннності. Вважаємо за доцільне на рис. 1.4 систематизувати перелік кіберзлочинів, які найчастіше вчиняються у віртуальному середовищі.

Рис. 1.4. Основні види кіберзлочинів

Джерело: власна авторська розробка

Відповідно до Конвенції про кіберзлочинність [27] на міжнародному рівні кіберзлочини поділяють на чотири групи:

1) злочинні діяння проти конфіденційності, цілісності та доступності комп’ютерних даних та інформаційних систем (незаконний доступ до даних,

несанкціоноване втручання у бази даних та в системи, нелегальне перехоплення інформації, зловживання пристроями);

2) злочинні діяння у сфері використання комп'ютерної техніки (підробка та шахрайські дії);

3) злочинні діяння, що пов'язані із змістом та контентом (створення та розповсюдження дитячої порнографії);

4) злочинні діяння, спрямовані на порушення авторських та суміжних прав.

М. Сащенко [28, с. 18] поглиблено дослідження та виокремлено ще одну групу кіберзлочинів, які зафіксовані в окремому протоколі, а саме злочинні діяння у віртуальному середовищі, що спрямовані на вчинення актів расизму та ксенофобії.

Однак, науковці не обмежуються такою класифікацією та доповнюють її пропозиціями поділяти кіберзлочини на такі, що потенційно небезпечні або насильницькі, до яких відносять кіберпереслідування, кібертероризм, кіберсталкінг, погрози фізичної розправи та дитячу порнографію, та на такі, що не містять ознак насильства, зокрема, розповсюдження вірусних програм, кібершахрайство, кіберкрадіжки, кібершпигунство, розповсюдження спаму та зловмисної реклами.

Варто зауважити, що достатньо часто використовуються такі методи кіберзлочинності, які спрямовані на пересічного користувача, зокрема:

1) фішинг (надсилання фейкових листів через електронну пошту, в яких розміщують прохання зазначити особисті дані або іншу конфіденційну інформацію);

2) злом (несанкціоноване та непогоджене втручання до пристрою користувачів із злочинним умислом);

3) натискання на оголошення (дозвіл користувача спрямувати його пристрій за певним посиланням, що дозволяє отримати зловмиснику доступ до нього);

4) шкідливе програмне забезпечення (спеціальна програма, що встановлюється на пристрій користувача без отримання не це його дозволу, яка чинить керований вплив та пристрій та його роботу).

Загрозливі тенденції поширення кіберзлочинності як глобального транскордонного явища потребує розроблення ефективної системи протидії, оскільки її наслідки відчутні як для розвитку держави, так і для суспільства. Відкритість державної інфраструктури для міжнародних розрахунків відкриває можливості для вчинення кіберзлочинів та легалізації активів, одержаних внаслідок протиправних діянь у кіберпросторі. Водночас, одержання швидкого доступу до інформаційних ресурсів й документального забезпечення у прихований спосіб дозволяє швидко приховати сліди вчиненого злочину та напрямки подальшого руху злочинно одержаних активів.

Достатньо вагомим наслідком кіберзлочинності являється дискредитація урядових структур окремих країн, що знижує їх імідж на міжнародній арені. В основному наслідки кіберзлочинності можна поділити на фінансові, що зумовлюють значні втрати банківських й фінансових установ та їх клієнтів, технологічні, які призводять до зростання витрат на придбання сучасних засобів захисту від кіберзлочинності, репутаційні та юридичні.

На сучасному етапі як на міжнародному, так і на національному рівні значні зусилля приділяються пошуку способів протидії кіберзлочинності, які істотно залежать від рівня розвитку країни та від динаміки кіберзлочинності у ній. Найбільш часто використовуваними способами боротьби із кіберзлочинами можна виділити наступні:

1) вдосконалення нормативно-правового забезпечення протидії кіберзлочинності;

2) чітке розмежування функцій та компетентностей правоохоронних органів у сфері протидії кіберзлочинності;

3) посилення практичної складової діяльності працівників підрозділів кіберполіції;

4) удосконалення методики проведення розслідувань кіберзлочинів;

5) налагодження міжвідомчої взаємодії на національному рівні та міжнародної співпраці.

Крім того, найбільш дієвими, на думку В. Кундеуса [29, с. 44.], є способи протидії кіберзлочинності, які передбачають кримінально-правовий вплив. В даному контексті, П. Баргіакчі [30] пропонує на міжнародному рівні узагальнити основні правила та принципи поведінки у віртуальному середовищі та уніфікувати загальну правову базу, що регулює відносини у кіберпросторі.

Не менш важливим залишається проведення спеціальних заходів щодо профілактики кіберзлочинності, які М. Сащенко [28, с. 18] пропонує реалізовувати у формі попереджувальної діяльності та координаційної діяльності правоохоронних та інших уповноважених державних органів, а також шляхом формування спеціальних програм протидії кіберзлочинності. Водночас, зважаючи на транснаціональний та транскордонний характер кіберзлочинності ефективна протидія даному деструктивному явищу повинна проводитися із залученням міжнародної спільноти.

Отже, дослідження кіберзлочинності як вагомого деструктивного явища соціально-економічного розвитку країни, дозволяють встановити, що кіберзлочинність являється окремим видом кримінальної діяльності, яка здійснюється з використанням кіберпростору з метою одержання прибутку або отримання доступу до інформації. Кіберзлочинність є надто розповсюдженою протиправною діяльністю, яка спрямовується на створення нових видів злочинів із використанням віртуального середовища. Наслідки кіберзлочинності є вагомими та зумовлюють деструктивні зміни як в економіці, так і в суспільстві.

Висновки до розділу 1

В умовах інтенсифікації розвитку цифрових технологій активізувалися процеси цифровізації економіки та суспільства, внаслідок чого значна кількість фінансових операцій здійснюється у віртуальному середовищі, яке є привабливим для вчинення протиправних діянь, пов’язаних із рухом тіньових капіталів. Встановлено, що посилення розвитку тіньового сектора економіки зумовлює зростання обсягів капіталів, які потребують узаконення та введення в офіційну економіку. Ефективним засобом досягнення бажаного протиправним структурам та злочинним організаціям вдається досягнути завдяки широкому використанні глобального цифрового простору. Окреслені тенденції свідчать про зростання ролі кіберзлочинності в сучасній світовій економічній системі та про її значний дестабілізуючий вплив на процеси і явища, що відбуваються в системі соціально-економічних відносин.

В процесі проведеного дослідження встановлено, що впродовж тривалого періоду часу проблема легалізації доходів, отриманих злочинним шляхом, як процесу узаконення тіньових капіталів, які здобуті внаслідок протиправних діянь, набуває вагомого значення та потребує розроблення комплексу заходів ефективної протидії даному масштабному й негативному явищу. При цьому, особливої гостроти набуває питання легалізації тіньових капіталів із використанням засобів цифрового зв’язку, що зумовлює стрімкий розвиток злочинності у кіберпросторі.

Доведено, що кіберзлочинність являється однією із вагомих проблем сьогодення та, зважаючи на постійне оновлення видів і способів вчинення кіберзлочинів, трансформується у транснаціональне й транскордонне явище, ефективна боротьба із яким потребує консолідації зусиль міжнародної спільноти.

РОЗДІЛ 2
ОЦІНКА СТАНУ ТА ТЕНДЕНЦІЙ ЩОДО ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

2.1. Аналіз обсягів легалізації доходів, отриманих у сфері кіберзлочинності, в Україні

Проблема легалізації злочинно отриманих активів актуалізувалася впродовж останніх років та обумовлена стрімким зростанням рівня тіньової економіки та появою нових дестабілізуючих чинників розвитку офіційного сектора економіки й суспільства. Систематичне накопичення нелегальних капіталів, що відбувається внаслідок ведення злочинної діяльності, доповнилося їх акумуляцією у віртуальному просторі через значне поширення кіберзлочинності. Як засвідчують результати досліджень Державної служби фінансового моніторингу України [31, с. 35] лише у 2021 р. вітчизняним підрозділом фінансової розвідки виявлено 13 фактів вчинення кіберзлочинів із використанням технологій заволодіння коштами суб'єктів господарської діяльності та узагальнено 19 матеріалів й 3 додатково узагальнених матеріалів, відносно яких виявлено підозри несанкціонованого доступу до фінансових ресурсів суб'єктів господарювання та списання або вчинення спроб списання з рахунків грошових коштів без відома та згоди клієнтів. При цьому, встановлена сума коштів, що були підготовлені для легалізації обчислюється у розмірі 71,6 млн. грн.

Результати проведених заходів кіберполіцією України щодо розслідування зазначених кіберзлочинів дозволили виявити основні шляхи такого несанкціонованого втручання, а саме:

1) застосування шкідливого програмного забезпечення;

2) злом електронних пошт з метою здійснення відправлення підроблених документів;

3) зумисне блокування sim-карт операторів мобільного зв'язку з метою їх подальшого перевипуску та одержання можливості входу до мобільного банкінгу;

4) неправомірне формування платіжних документів, що здійснюється із різних IP-адрес;

5) віддалене управління рахунком «Клієнт–Банк» та використання послуги «Мобільний банкінг»;

6) широке застосування сервісів, за допомогою яких здійснюються грошові перекази: Western Union, TransferWise, MoneySend, MoneyGram.

При цьому, найчастіше використовувалися такі інструменти як готівка, фінансово допомога, використання платіжних карток, товари та надання різних послуг, міжнародні перекази.

Вважаємо за необхідне висвітлити основні схеми здійснення типових кіберзлочинів. Оскільки, питому вагу серед кіберзлочинів в Україні займає здійснення хакерських атак з метою заволодіння коштами підприємств-нерезидентів, то поглибимо їх дослідження і на рисунку 2.1 систематизуємо схему здійснення кіберзлочинів із використання шахрайства щодо заволодіння коштами підприємств-нерезидентів.

Даний вид кіберзлочинів передбачає здійснення хакерських атак, внаслідок яких із рахунків підприємства А, що є нерезидентом, списуються кошти на рахунок іншого підприємства, який розміщено у Банку 1. Грошові кошти в швидкому режимі транзитом переміщуються від підприємства-нерезидента А на рахунки групи підприємств в інших банках. Причому, рахунок в банку відкривається незадовго до здійснення нелегальної операції, тому банк не має змоги зв'язатися з таким клієнтом. Одночасно на рахунок підприємства, де було списано кошти внаслідок хакерської атаки, що відкритий в Банку 2, зараховано кошти від підприємства-нерезидента Б, а також отримано запит від іноземного банку про шахрайські дії цього ж підприємства.

Рис. 2.1. Схема здійснення кіберзлочинів із використання шахрайства щодо заволодіння коштами підприємств-нерезидентів

Джерело: складено автором за даними [31, с. 36]

В подальшому, злочинно одержані кошти переведено на рахунки фіктивних підприємств, окремі із яких мають ознаки здійснення кримінальної діяльності. Крім того, по відношенню до підприємства, що зазнало хакерської атаки, встановлено декількаразову зміну назви, а інформація щодо задекларованих валових доходів та сплачених податків відсутня в базах даних.

Другим найбільш розповсюдженим кіберзлочином є незаконне зумисне заволодіння активами та грошовими коштами підприємства-нерезидента, що здійснюється шляхом несанкціонованого протиправного списання коштів з рахунків.

Алгоритм здійснення такого кіберзлочину (рис. 2.2) полягає у спеціальному створені нового суб'єкта господарювання, який здійснює

перерахунок коштів із особистого рахунку, відкритого у Банку А на такий же власний рахунок в Банку Б. Виявлено, що в Банку А операції здійснювалися на підставі сфальсифікованого зовнішньоекономічного контракту та інших документів, що підтверджують джерело походження коштів суб'єкта господарювання. При цьому, митні органи не можуть підтвердити факт експорту товарів, які, до слова, не є вироблені даним господарюючим суб'єктом.

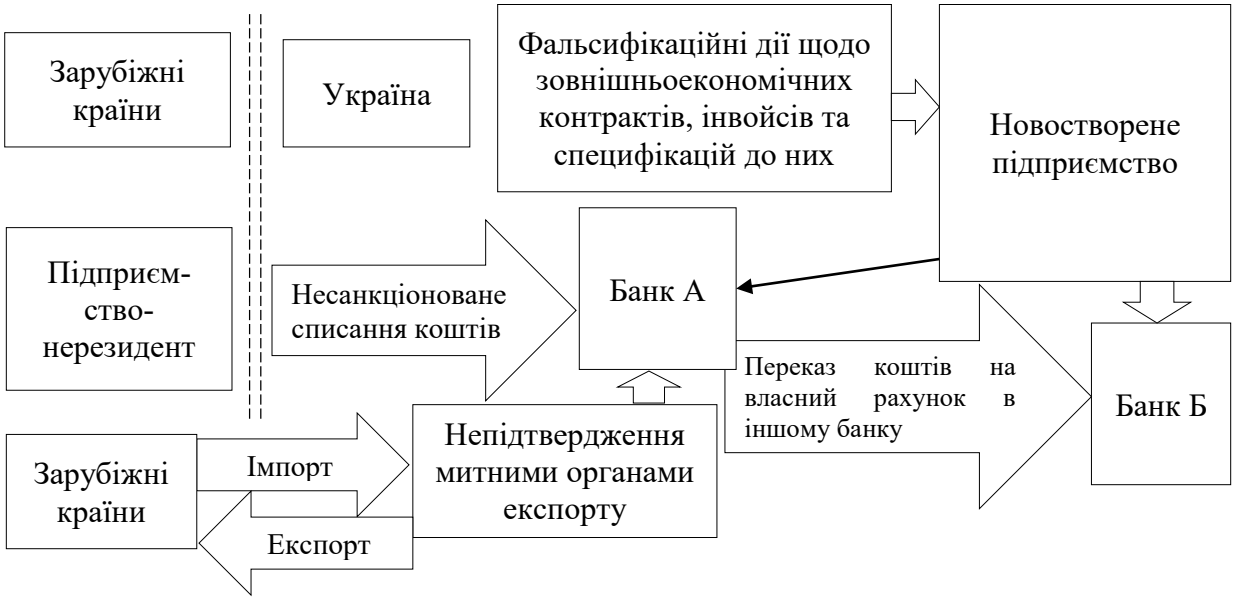


Рис. 2.2. Схема здійснення кіберзлочинів через несанкціоноване заволодіння активами шляхом несанкціонованого списання коштів підприємств-нерезидентів

Джерело: складено автором за даними [31, с. 36]

Не менш вагомого значення в системі кіберзлочинності набуває здійснення списання в незаконний спосіб коштів з банківських рахунків через дистанційне керування. Такий вид кіберзлочинів передбачає вчинення шахрайських дій та впродовж короткого терміну переведення значних сум на рахунок однієї фізичної особи. Типологічну схему здійснення такого виду кіберзлочину відобразимо на рис. 2.3.

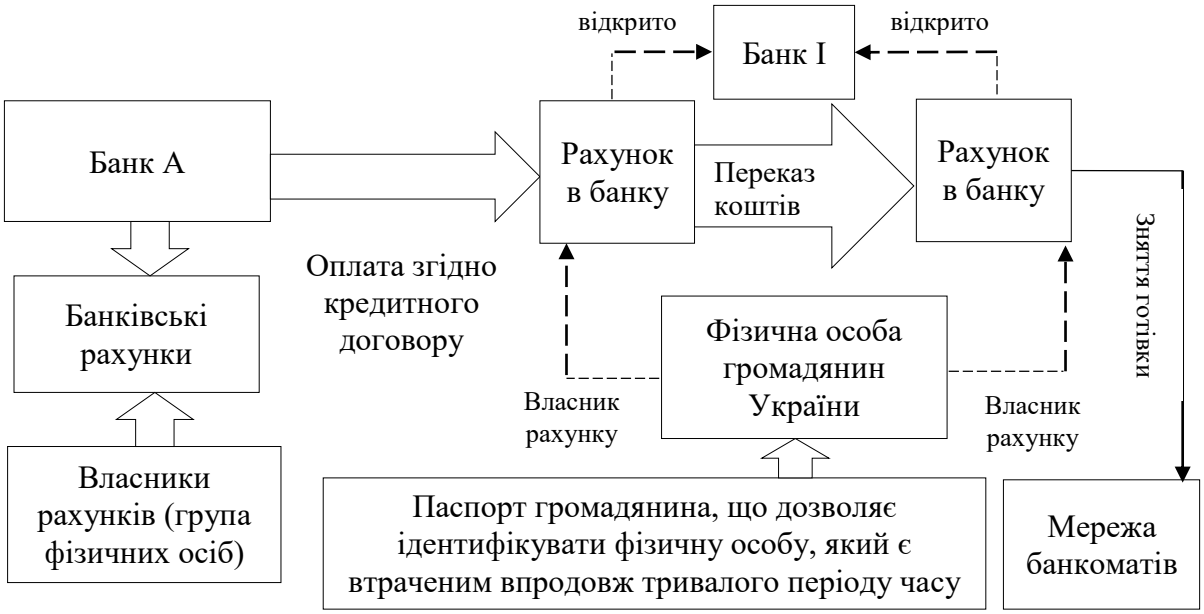


Рис. 2.3. Схема здійснення кіберзлочинів шляхом незаконного списання грошових коштів з банківських рахунків через дистанційне керування

Джерело: складено автором за даними [32]

Сутність зазначеного злочинного діяння у кіберпросторі полягає у здійсненні шахрайства із фінансовими ресурсами через їх списання з рахунків із дистанційним керуванням. Впродовж короткого періоду часу зловмисник із рахунків декількох фізичних осіб під виглядом оплати за кредитним договором списав значні суми коштів та перерахував їх на рахунок однієї фізичної особи, які переміщено на інший рахунок у тому ж банку та, в подальшому, знято із використанням мережі банкоматів.

Очевидно, що банк, в якому відкриті рахунки групи фізичних осіб, подав звернення до банку, куди були спрямовані кошти, про вчинення шахрайських дій, внаслідок чого встановлено, що відкриті рахунки мають віддалений доступ керування із використанням однієї і тої ж IP–адреси. Крім того, виявлено, що документ, на підставі якого здійснюється ідентифікація особи-зловмисника, був втрачений декілька років тому та визнаний втраченим.

В цілому, оцінюючи загрози кіберзлочинності в Україні, необхідно звернути увагу та їх зростаючий характер та на вагомий вплив на систему протидії легалізації доходів, отриманих злочинним шляхом. Зважаючи на

вагому роль зростання кіберзлочинності в антилегалізаційній системі, вважаємо за доцільне прослідкувати динаміку обсягів коштів, які щорічно легалізовуються в Україні (рис. 2.4), що дозволить оцінити вагомість аналізованої проблеми.

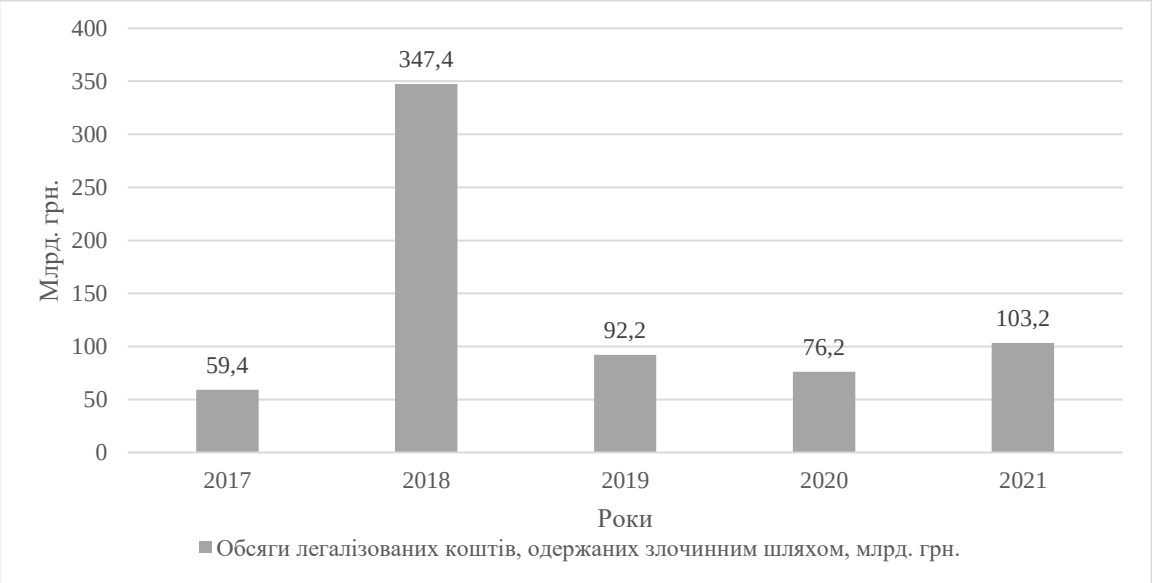


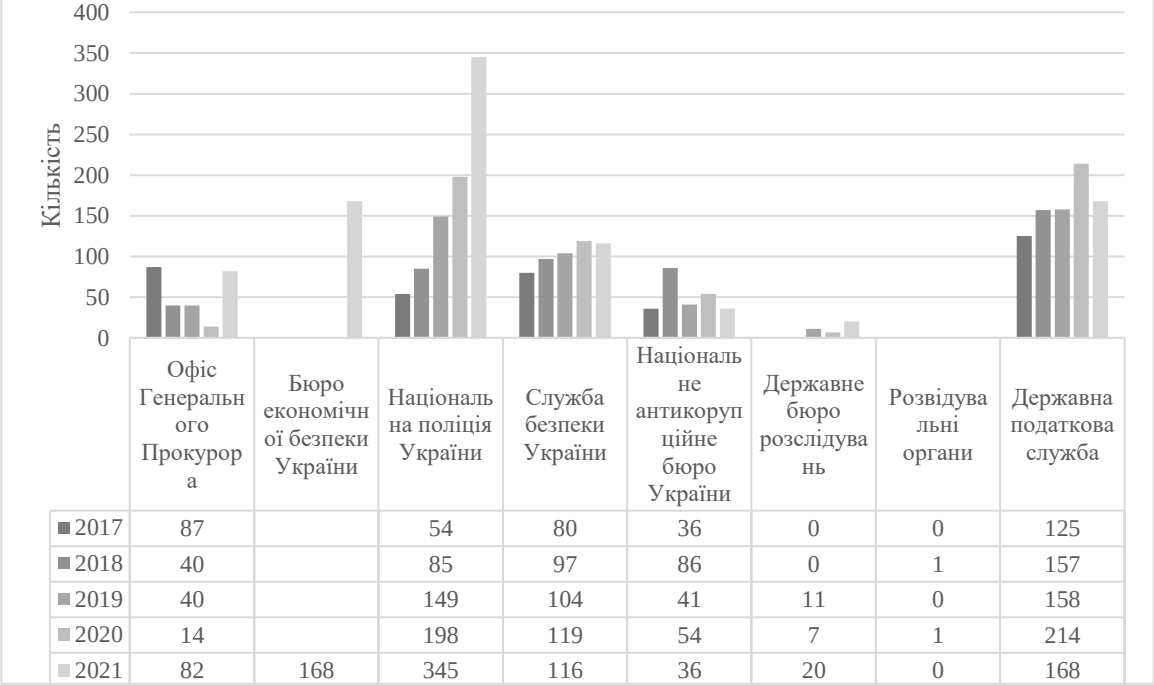
Рис. 2.4. Динаміка обсягів легалізованих (відмитих) коштів, що були отримані внаслідок злочинних діянь в Україні у 2017–2021 рр.

Джерело: складено автором за даними: [31, с. 8; 33, с. 8; 34, с. 25; 35, с. 27; 36, с. 6]

Проведені дослідження засвідчують, що впродовж 2017–2021 рр. обсяги легалізованих тіньових капіталів мають тенденції до зростання, особливо критичні обсяги зафіксовано у 2018 р. (347,4 млрд. грн. за рік), що на 484,85 % більше у порівнянні із 2017 р. У 2019 р. спостерігається значне зниження значення аналізованого показника до 92,2 млрд. грн. та у 2020 р. до 76,2 млрд. грн. Проте, дестабілізуючі чинники пандемії COVID-19 у 2021 р. стимулювали посилення злочинності у сфері легалізації протиправних капіталів, що доводить зростання обсягів легалізованих коштів до 103,2 млрд. грн. (на 35,43 %).

При цьому, необхідно відзначити достатньо високий рівень професіоналізму Державної служби фінансового моніторингу України щодо виявлення підозрілих операцій, що можуть містити ознаки легалізаційної

діяльності, зокрема й у кіберпросторі. Якщо проаналізувати кількість переданих Держфінмоніторингом матеріалів до правоохоронних та розвідувальних органів впродовж 2017–2021 рр. (рис. 2.5), то можна помітити, що найбільш питому вагу має міжвідомча взаємодія із Національною поліцією України, Державною податковою службою та Службою безпеки України.



	Офіс Генерального Прокурора	Бюро економічної безпеки України	Національна поліція України	Служба безпеки України	Національне антикорупційне бюро України	Державне бюро розслідувань	Розвідувальні органи	Державна податкова служба
2017	87		54	80	36	0	0	125
2018	40		85	97	86	0	1	157
2019	40		149	104	41	11	0	158
2020	14		198	119	54	7	1	214
2021	82	168	345	116	36	20	0	168

Рис. 2.5. Динаміка кількості матеріалів, сформованих Держфінмоніторингом та переданих до правоохоронних та розвідувальних органів у 2017–2021 рр.

Джерело: складено автором за даними: [31, с. 38; 33, с. 48; 34, с. 39; 35, с. 36; 36, с. 38]

Причому, у 2021 р. спостерігається різке зростання кількості переданих матеріалів до Національної поліції України, а саме 345 матеріалів, що на 74,24 % більше, ніж у 2020 р. Зауважимо, що значна частка із виявлених Держфінмоніторингом підозрілих операцій пов’язані із вчиненням злочинів у кіберпросторі, що доводить вагомість дослідження кіберзлочинності в Україні та обсягів легалізованих коштів, отриманих внаслідок вчинення кіберзлочинів.

Таким чином, проведений аналіз обсягів легалізації доходів, отриманих у сфері кіберзлочинності, в Україні дозволяє виявити активізацію діяльності злочинців у кіберпросторі та формування ними нових схем вчинення кіберзлочинів, серед найпоширеніших із яких можна виокремити використання шахрайства щодо заволодіння коштами підприємств-нерезидентів, несанкціоноване заволодіння активами шляхом несанкціонованого списання коштів підприємств-нерезидентів та незаконне списання грошових коштів з банківських рахунків через дистанційне керування. Встановлено, що суми легалізованих коштів, отриманих у сфері кіберзлочинності досягають позначки у 71,6 млн. грн. щорічно.

2.2. Оцінка динаміки кіберзлочинності в Україні

Інтенсифікація розвитку новітніх інформаційних технологій та їх запровадження в економіку й суспільство спричинює проблему їх залучення до вчинення протиправних діянь й порушення інтересів у різних сферах діяльності. Віртуальне цифрове середовище надає беззаперечні можливості для його використання в злочинних цілях, адже розширює свободу дій, забезпечує конфіденційність діянь та високий рівень захисту. Такі умови являються надзвичайно комфортними для активізації діяльності кіберзлочинців. Безумовно, розвиток кіберзлочинності є одним із напрямів інтенсифікації кримінальної діяльності, що становить значну загрозу на національному та глобальному рівнях, а ефективна боротьба із кіберзлочинністю переміщується на передній план та становиться пріоритетною для державних правоохоронних органів.

Як засвідчують оприлюднені Національною поліцією України дані, впродовж 2017–2021 рр. спостерігається стрімке зростання кількості вчинених кіберзлочинів (рис. 2.6) із 4500 злочинів у 2017 р. до 10020 злочинів у 2021 р. (темп росту становить 122,67 %). Очевидно, що посилення кіберзлочинності у

2020–2021 рр. зумовлено послабленням соціальної активності населення та карантинними обмеженнями, які запроваджені з метою запобігання поширенню пандемії COVID-19 та поступовим переходом на здійснення електронних розрахунків.

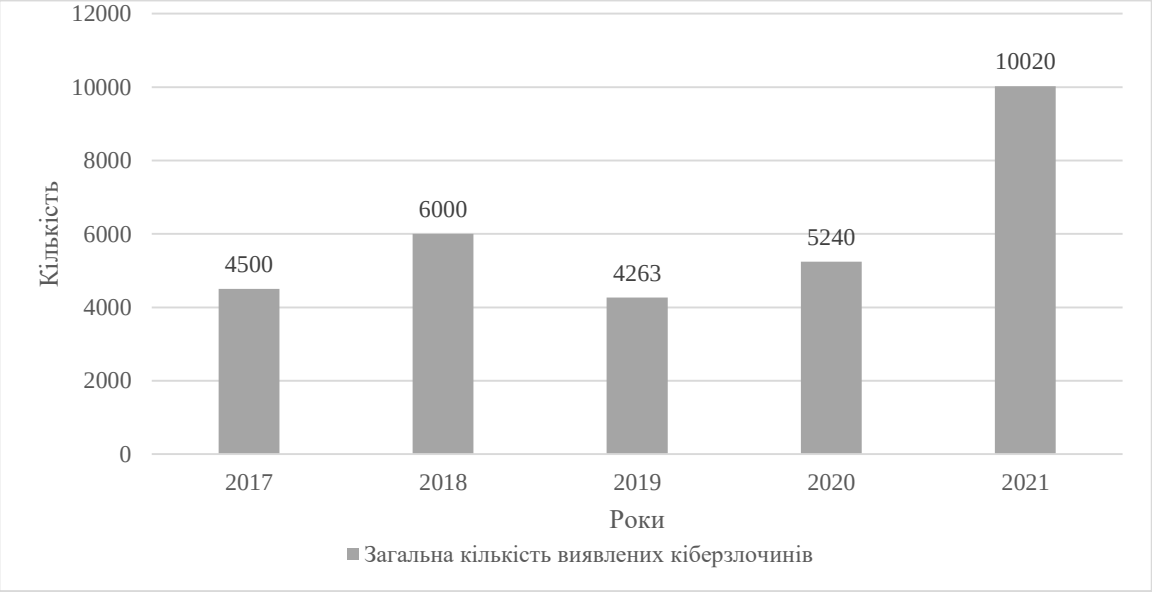


Рис. 2.6. Динаміка загальної кількості виявлених в Україні кіберзлочинів у 2017–2021 рр.

Джерело: складено автором за даними [37, с. 13; 38, с. 14; 39, с. 9; 40, с. 12; 41, с. 16]

Водночас, варто проаналізувати динаміку кіберзлочинності в розрізі сфер вчинення таких протиправних діянь. На рис. 2.7 відобразимо основні тенденції виявлених кіберзлочинів у банківській сфері, у сфері комп'ютерних систем та тих кіберзлочинів, що пов'язані із онлайн шахрайством.

Результати проведеного аналізу дозволяють виявити, що найбільша кількість кіберзлочинів вчинена у банківській сфері, зокрема: 1330 злочинів у 2017 р., 2398 злочинів у 2018 р., 1641 злочин у 2019 р., 2110 злочинів у 2020 р. та 3049 злочинів у 2021 р. Дещо нижчі, проте, достатньо вагомі обсяги кіберзлочинів спостерігаються у сфері комп'ютерних систем та ще нижчі – у сфері онлайн шахрайства. При цьому, значне зростання щодо вчинення кіберзлочинів усіх аналізованих видів зафіксовано у 2021 р.

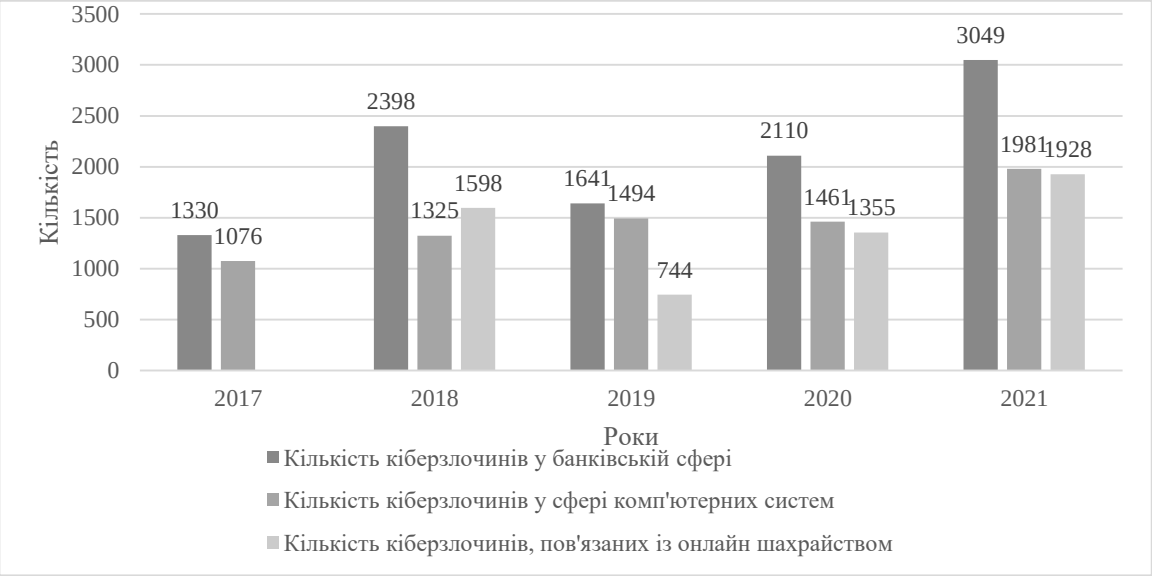


Рис. 2.7. Динаміка кількості виявлених в Україні кіберзлочинів відповідно до сфери діяльності у 2017–2021 рр.

Джерело: складено автором за даними [37, с. 14; 38, с. 13; 39, с. 9; 40, с. 12; 41, с. 16]

Варто зазначити, що особливо гостро постала проблема зростання випадків онлайн шахрайства, що зафіксовано на рівні 42,3 %, відсоток розкриття яких становить 80 %. Така ситуація підтверджує складність виявлення, розслідування та розкриття даного виду кіберзлочинів, що обґрунтовують більшість із науковців.

Не менш загрозливою є ситуація щодо створення та поширення вірусів. Результати проведених досліджень в даному напрямку дозволяють виявити транснаціональну компоненту такого роду кіберзлочинів, що доводить високий рівень міжнародної взаємодії в напрямку виявлення кіберзлочинності. Залучення правоохоронних органів зарубіжних країн та співпраця на міжнародному рівні дозволили виявити 3 осіб із України, які брали участь у створені вірусу «EMOTET», що завдали сумарних збитків обсягом понад 2 млрд. дол. США. Іншим достатньо вагомим злочином у кіберпросторі встановлено діяльність над створенням такого шкідливого програмного забезпечення як «Ransomware», внаслідок чого сумарні збитки

суб'єктам господарювання США та Кореї завдані у обсягах понад 500 млн. дол. США.

Проблема інтенсифікації кіберзлочинності потребує негайного вирішення не лише в Україні, адже операції, що здійснюються у віртуальному середовищі дедалі частіше піддаються несанкціонованому сторонньому втручанню злочинців та злочинних угрупувань. Свідченням цього являється вагома увага міжнародної спільноти до проведення розрахунків та пошуку ефективних методів забезпечення кібербезпеки, оцінювання рівня якої проводиться на підставі обчислення Глобального індексу кібербезпеки, що передбачає оцінювання країни за такими параметрами як здатність виявляти кіберзагрози, створення дієвої системи безпеки кіберпростору та розвиток освіти у сфері кібербезпеки й посилення кіберграмотності населення.

Зважаючи на наявність в Україні негативних тенденцій щодо поширення кіберзлочинності, вважаємо за доцільне прослідкувати динаміку Глобального індексу кібербезпеки та провести порівняльні оцінювання його значення із окремими країнами світу. На рис. 2.8 відобразимо динаміку Глобального індексу кібербезпеки в Україні у 2017–2021 рр.

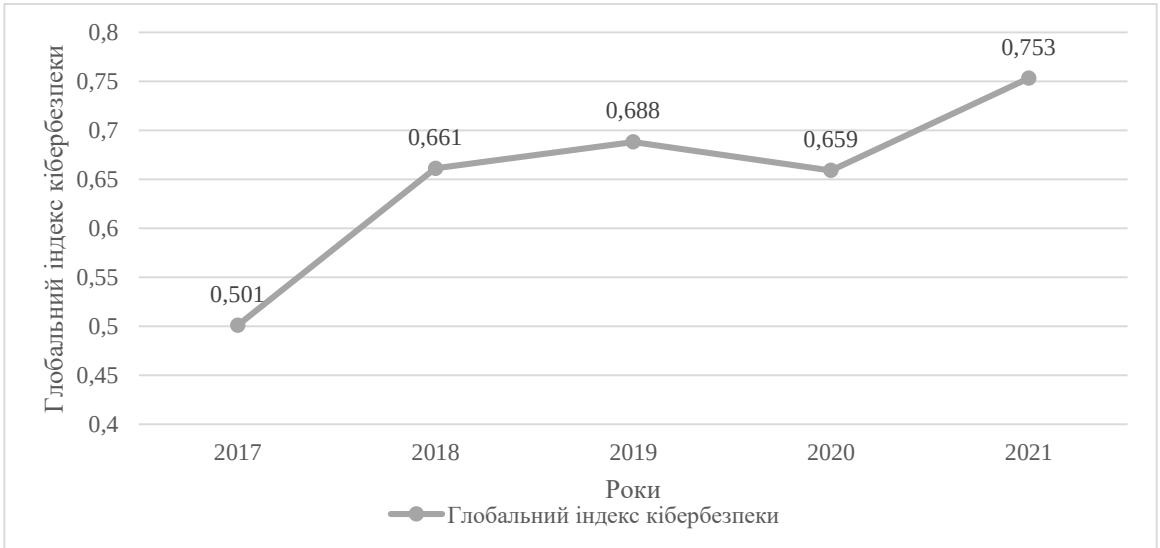


Рис. 2.8. Динаміка Глобального індексу кібербезпеки в Україні у 2017–2021 рр.

Джерело: складено автором за даними [42–46]

Результати проведеного аналізу дозволили побудувати зростаючий тренд щодо Глобального індексу кібербезпеки в Україні, що доводить необхідність підвищення уваги до вирішення проблеми захисту інформаційних ресурсів у кіберпросторі. Однак, варто зауважити, що в умовах 2020 р. значення аналізованого показника дещо знизилося із 0,688 до 0,659, що говорить про послаблення можливостей країни протистояти викликам і загрозам у віртуальному середовищі. Водночас, під впливом поширення пандемії COVID-19 активізувалися процеси вчинення таких кіберзлочинів як дрібне шахрайство, за рахунок чого зросли обсяги загальної кількості протиправних діянь у кіберпросторі та, відповідно, зниження рівня кібербезпеки. У 2021 р. після вжиття відповідних заходів рівень кібербезпеки вдалося підняти до 0,753.

Проте, порівнюючи динаміку зміни Глобального індексу кібербезпеки в Україні з країнами Європейського Союзу та іншими зарубіжними країнами, відмічаються достатньо низькі позиції щодо аналізованого показника в України. На рис. 2.9 вважаємо за необхідне систематизувати дані щодо динаміки Глобального індексу кібербезпеки в країнах Європейського Союзу та в окремих зарубіжних країнах.

З одержаних даних видно, що найбільш захищеною країною щодо діяльності у кіберпросторі є США, Глобальний індекс кібербезпеки яких максимально наближений до 1. Достатньо високі значення аналізованого показника позиціонують Великобританія, Японія та Корея, які також фіксують достатньо високі значення Глобального індексу кібербезпеки. Водночас, високо розвинуті країни Європейського Союзу спроможні також досягнути високого рівня кібербезпеки (Австрія, Бельгія, Данія, Іспанія, Нідерланди, Німеччина, Португалія, Фінляндія, Франція), а найнижчі значення присутні у тих країнах, які нещодавно завершили процеси трансформаційної перебудови (Румунія, Угорщина, Болгарія, Словенія, Кіпр та Мальта).

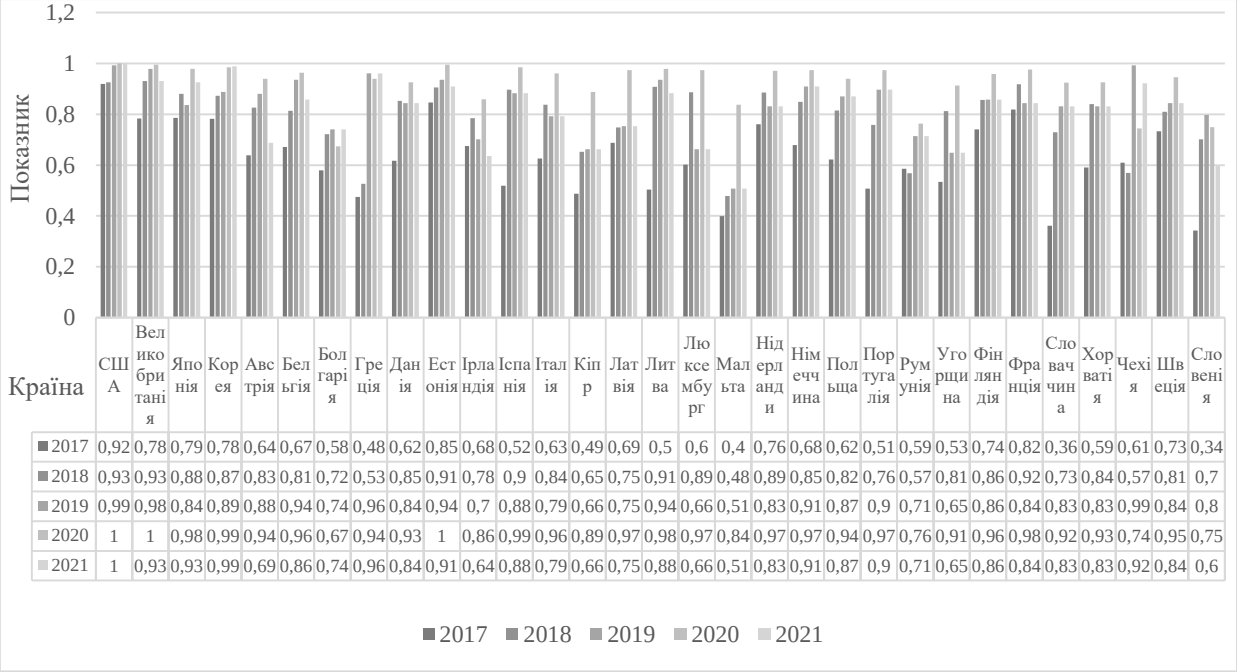


Рис. 2.9. Динаміка Глобального індексу кібербезпеки в країнах Європейського Союзу та в інших країнах світу у 2017–2021 рр.

Джерело: складено автором за даними [42–46]

Поглиблені дослідження щодо забезпечення кібербезпеки, проведені шляхом групування країн обраної для аналізу групи з використанням спеціального програмного забезпечення Statistica, дозволяють виявити три однорідні групи країн, які характеризуються спільними ознаками (таблиця 2.1).

Таблиця 2.1

Групування країн світу за показником Глобального індексу кібербезпеки у 2017–2021 рр.

№ за/п	Країна	Група			
1.	США	1	21.	Греція	2
2.	Великобританія		21.	Португалія	
3.	Японія		22.	Словаччина	
4.	Корея		23.	Чехія	
5.	Австрія		24.	Болгарія	3
6.	Бельгія		25.	Ірландія	
7.	Данія		26.	Кіпр	
8.	Естонія		27.	Люксембург	
9.	Іспанія		28.	Мальта	
10	Італія		29.	Румунія	

Продовження табл. 2.1

11.	Латвія	1	30.	Угорщина	3
12.	Литва		31.	Словенія	
13.	Нідерланди		32.	Україна	
14.	Німеччина				
15.	Польща				
16.	Фінляндія				
17.	Франція				
18.	Хорватія				
19.	Швеція				

Джерело: складено автором за даними [42–46]

До першої групи увійшли США, Великобританія, Японія, Корея, Австрія, Бельгія, Данія, Естонія, Іспанія, Італія, Латвія, Литва, Нідерланди, Німеччина, Польща, Фінляндія, Франція, Хорватія та Швеція, які забезпечують високий рівень протидії викликам, загрозам та небезпекам у кіберпросторі, та зуміли налагодити тісну співпрацю на міжнародному рівні щодо боротьби з кіберзлочинністю.

До другої групи належать Греція, Португалія, Словаччина та Чехія, де зафіксовано посередній рівень боротьби з кіберзлочинністю та протидії кіберзагрозам. Третю групу складають Болгарія, Ірландія, Кіпр, Люксембург, Мальта, Румунія, Угорщина, Словенія, більшість із яких характеризуються як країни пострадянського простору, що піддаються значному дестабілізуючому впливу вагомих факторів. Крім того, до даної групи увійшла Україна, яка також позиціонується як країна, що не спроможна належним чином протистояти кібервикликам та кіберзагрозам.

Очевидно, що в Україні та в низці зарубіжних країн проблеми кіберзлочинності присутні та загострюються дестабілізуючими чинниками сучасності. Водночас, варто констатувати, що на міжнародному рівні значні зусилля спрямовуються на захист кіберпростору та на зниження рівня злочинності у віртуальному середовищі. Достатньо великі обсяги ресурсів спрямовуються на розроблення інноваційних технічних засобів захисту та протидії кіберзлочинам, а також на створення відповідного програмного забезпечення. Результати проведених досліджень дозволили з’ясувати, що

впродовж 2017–2021 рр. на забезпечення безпеки у кіберпросторі спрямовувалися колосальні суми грошових коштів, динаміку яких відобразимо на рис. 2.10.

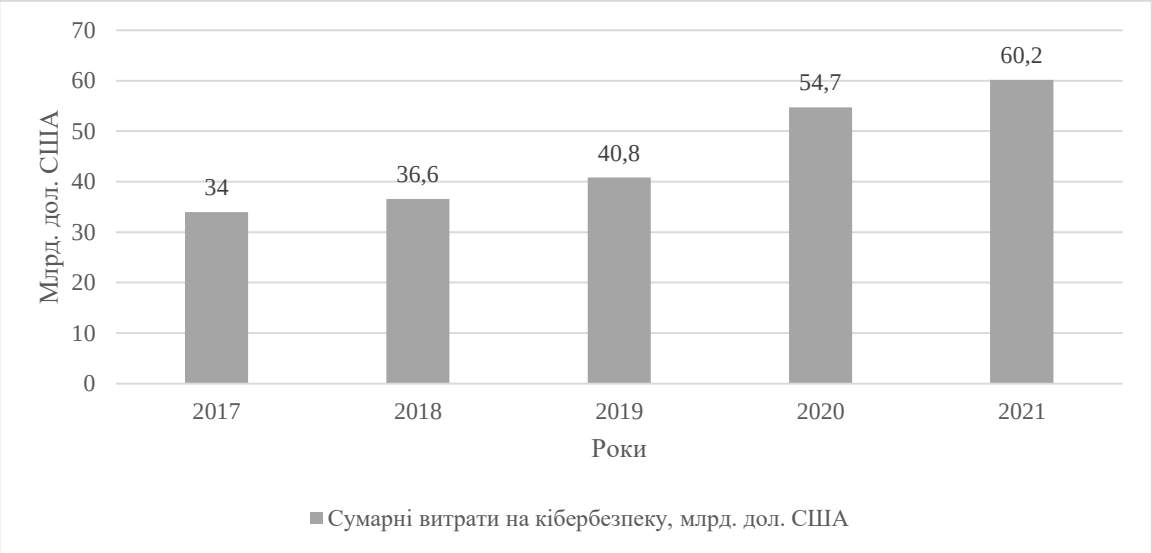


Рис. 2.10. Динаміка сумарних витрат на кібербезпеку в країнах світу у 2017–2021 рр.

Джерело: складено автором за даними [47]

Починаючи із 2017 р. щорічно на створення засобів захисту інформації у кіберпросторі та на запобігання кіберзлочинам спрямовується понад 30 млрд. дол. США, зокрема, у 2017 р. 34 млрд. дол. США, у 2018 р. 36,6 млрд. дол. США, у 2019 р. 40,8 млрд. дол. США, у 2020 р. 54,7 млрд. дол. США, а у 2021 р. даний показник досягнув позначки у 60,2 млрд. дол. США. Проте, подолати проблему інтенсифікації кіберзлочинності ні на національному, ні на міжнародному рівні досі не вдалося, а існуючі заходи не дають бажаного економічного ефекту, що свідчить про нагальну потребу поглиблення досліджень та вивчення зазначеної проблематики.

Отже, проведені оцінки динаміки кіберзлочинності в Україні впродовж 2017–2021 рр. дозволили виявити її зростаючий характер та потребу розроблення ефективної системи протидії кіберзлочинам.

Висновки до розділу 2

Проблема легалізації доходів, отриманих у сфері кіберзлочинності, в Україні набуває особливої вагомості в умовах посилення впливу зовнішніх і внутрішніх викликів й небезпек та інтенсифікації розвитку кіберзлочинності. Результати проведених емпіричних досліджень обсягів легалізації доходів, отриманих у сфері кіберзлочинності, в Україні дозволили виявити низку типових схем, за допомогою яких вчиняються кіберзлочини, зокрема: використання шахрайства щодо заволодіння коштами підприємств-нерезидентів, несанкціоноване заволодіння активами шляхом несанкціонованого списання коштів підприємств-нерезидентів, незаконне списання грошових коштів з банківських рахунків через дистанційне керування.

Встановлено, що найбільші обсяги легалізованих (відмитих) коштів, отриманих внаслідок злочинних діянь у тіньовому секторі економіки України зафіксовано у 2018 р. – 347,4 млрд. грн. Подальші періоди мають тенденції до зниження, проте, у 2021 р. знову спостерігається зростання обсягів коштів, що виведені із тіні.

Виявлено активізацію діяльності Державної служби фінансового моніторингу України щодо антилегалізаційної діяльності, про що свідчить посилення її взаємодії із правоохоронними органами. Варто відмітити, що найбільша кількість матеріалів, які мають ознаки відмивання нелегальних активів, передано до Державної податкової служби України та Національної поліції України.

Доведено зростання загальної кількості виявлених в Україні кіберзлочинів, обсяги яких у 2021 р. досягнули позначки у 10020 злочинів, питома вага вчинення яких зосереджена у банківській сфері. При цьому, встановлено, що при зростаючому тренді Глобального індексу кібербезпеки в умовах 2021 р. в Україні активізувалася кіберзлочинність у сфері комп’ютерних систем та онлайн шахрайства.

РОЗДІЛ 3
СТРАТЕГІЧНІ ПРІОРИТЕТИ ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

3.1. Напрями удосконалення національної системи протидії кіберзлочинності

Прогресивний розвиток інформаційних технологій та прагнення України реалізувати політику цифровізації економіки й суспільства призвели до появи нового напряму кримінальної діяльності – кіберзлочинності. Транснаціональний характер даного деструктивного явища та його стрімке поширення провокують необхідність формування ефективної системи запобігання та протидії вчиненню кіберзлочинів, оскільки щорічні збитки від кіберзлочинності на світовому рівні складають понад 1,5 трлн. дол. США [48].

Зауважимо, що кіберзлочинність почала інтенсивно розвиватися порівняно недавно, проте набула світового значення та перетворилася на одну із найнебезпечніших міжнародних загроз. Поява нових методів й способів вчинення кіберзлочинів та їх видів, а також набуття ними транскордонного характеру вимагає належної реакції світового співтовариства у даній сфері. Першочергове значення в даному контексті має розроблення ефективних норм міжнародного права, спроможних врегулювати відносини у сфері кіберзлочинності, вчасно виявляти кіберзлочини та ефективно протидіяти протиправним діянням з використанням цифрових технологій у віртуальному середовищі.

Зважаючи на зростаючі масштаби кіберзлочинності, світовою спільнотою актуалізується проблема прийняття відповідних законодавчих та нормативно-правових документів з метою формування структурованого й зрозумілого інформаційного простору, спроможного забезпечити високий рівень конфіденційності та достовірності інформаційних потоків, збереження авторських прав, досягнення високого ступеню захисту від шахрайських дій.

Очевидно, що одним із пріоритетних завдань як на міжнародному, так і на національному рівні щодо захисту інтересів економічних агентів у кіберпросторі, є забезпечення достатнього рівня кібербезпеки, оскільки питома вага кіберзлочинності постійно зростає, а інноваційний розвиток інформаційних технологій та їх поступова конвергенція із технологіями штучного інтелекту посилює не лише сталий розвиток економіки й суспільства, а й призводить до значних деструктивних змін. Проблема запобігання та протидії кіберзлочинності в Україні особливо гостро постала в період поширення пандемії COVID-19 та в умовах військового протистояння збройній агресії Російської Федерації, адже значна чисельність фінансових операцій трансформувалися у віртуальний простір та здійснюються за допомогою цифрових технологій, а Російська Федерація являється основним джерелом загроз кібербезпеці не лише України, а всієї міжнародної спільноти. Оцінюючи дані кризові для України періоди, вдається встановити, що зростаючі темпи поширення кіберзлочинності припадають саме на 2020–2022 рр., що потребує формування комплексу заходів, за допомогою яких вдасться мінімізувати негативний вплив та забезпечити високий рівень безпеки функціонування кіберпростору та здійснення фінансових операцій у віртуальному середовищі.

В даному контексті першочергового значення набуває поглиблення вивчення питання захисту національних інтересів України у кіберпросторі, що відповідає концепції забезпечення кібербезпеки держави. Створення ефективної системи забезпечення кібербезпеки дозволить зміцнити позиції країни на міжнародній арені та довести спроможність протистояти зовнішнім і внутрішнім викликам сучасності. На рис. 3.1 пропонуємо відобразити пропоновану систему забезпечення кібербезпеки держави, сформовану із урахуванням впливу на неї кіберризиків та кіберзагроз, завдань функціонування національної системи протидії кіберзлочинності та принципів її забезпечення.

Рис. 3.1. Система забезпечення кібербезпеки держави

Джерело: власна авторська розробка

Безумовно, посилення негативного впливу кіберризиків та кіберзагроз, а також удосконалення інструментів їх реалізації спостерігатиметься і в стратегічній перспективі, що обумовлює необхідність та значимість їх максимально швидкого виявлення й мінімізації. Не менш важливим за таких умов є реалізація Стратегії кібербезпеки України [49], яка покликана створити належні умови для безпечного функціонування кіберпростору та вчасного виявлення кіберзагроз.

Необхідність удосконалення національної системи протидії кіберзлочинності обґрунтовується потребою посилення боротьби із кіберзлочинністю, яка поширюється надшвидкими темпами та деструктивно впливає на суспільно-політичні та соціально-економічні процеси, чим знижує

рівень довіри громадян до цифрових технологій. Водночас встановлено, що кіберпростір широко використовується для легалізації тіньових доходів, походження яких має протиправний, а подекуди й кримінальний характер. Вважаємо за доцільне на рис. 3.2 систематизувати основні напрямки протидії кіберзлочинності в Україні.

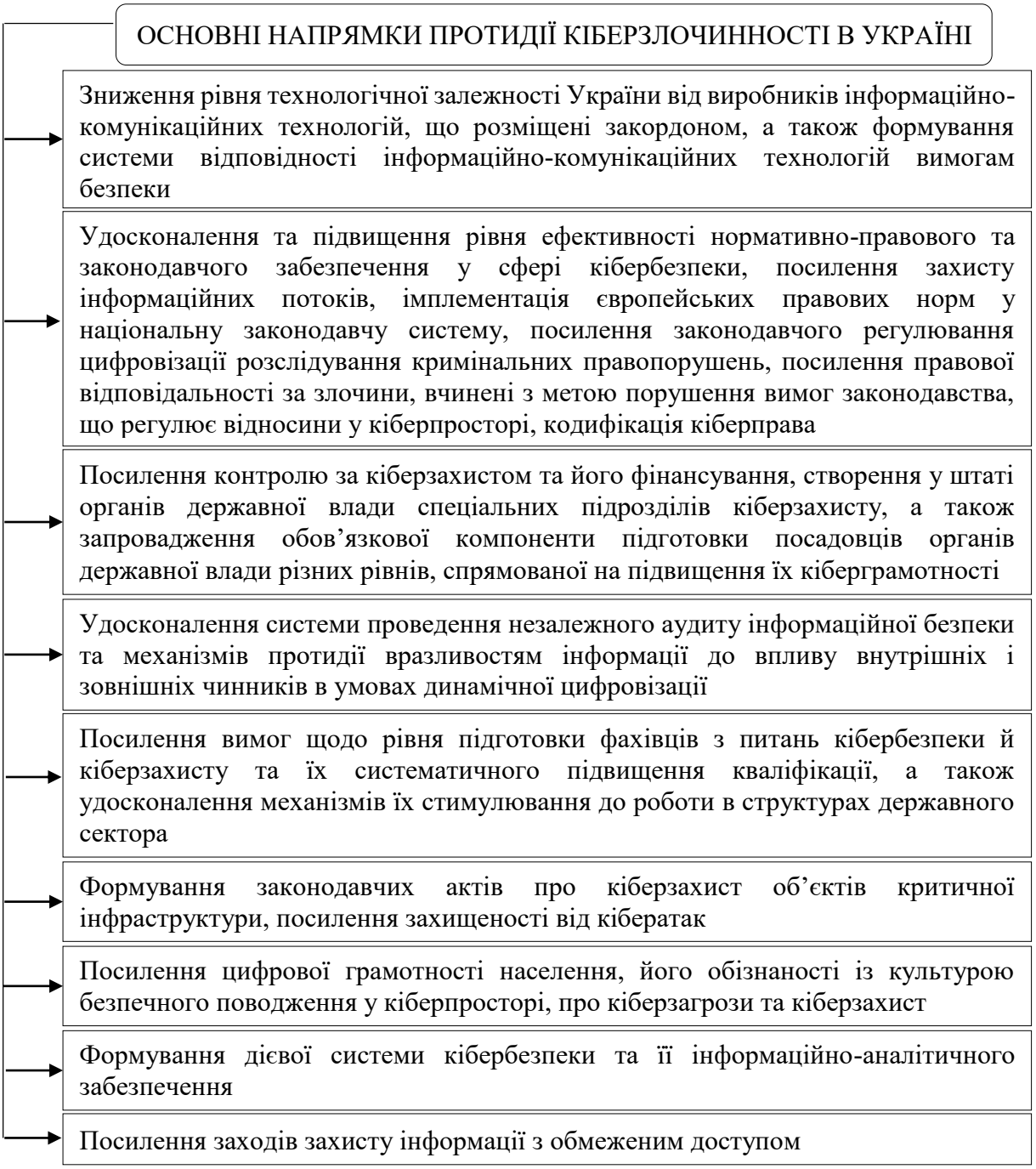


Рис. 3.2. Основні напрямки протидії кіберзлочинності в Україні

Джерело: складено автором за даними [49]

Зауважимо, що серед основних напрямків протидії кіберзлочинності в Україні варто виділити необхідність удосконалення чинного законодавства та приведення його у відповідність із нормами міжнародного права у сфері кіберзахисту та регулювання взаємовідносин у кіберпросторі; посилення організаційного механізму захисту інформаційних потоків у кіберпросторі та посилення уваги щодо підготовки фахівців, що здійснюють діяльність щодо забезпечення кібербезпеки та кіберзахисту. Вагомим здобутком в напрямку удосконалення національної системи протидії кіберзлочинності може стати формування механізму кодифікація кіберправа.

Водночас, ескалація військового конфлікту України із Російською Федерацією, який трансформувався у повномасштабне вторгнення країни-агресора на територію України, створив необхідність захисту національних інтересів України від злочинного стороннього впливу. При цьому, відмічається активізація діяльності зловмисників у кіберпросторі, внаслідок чого їх зусилля спрямовуються на виникнення загроз, що зумовлюють потребу захисту територіальної цілісності та суверенітету країни, прав, свобод та інтересів населення у кіберпросторі, а також посилення європейської та євроатлантичної інтеграції України у сфері кібербезпеки.

Досягнення бажаного результату щодо протидії кіберзлочинності в Україні стає можливим при скоординованій діяльності органів державної влади усіх рівнів, суспільства та міжвідомчої й міжнародної взаємодії спеціалізованих державних органів й міжнародних організацій. Водночас, вагомого значення набуває формування ефективної системи забезпечення кібербезпеки держави. Крім того, обмежуватися поточними заходами недостатньо, а потрібно спрямовувати значні зусилля на формування стратегічних пріоритетів забезпечення кіберзахисту та зміцнення кібербезпеки. Основні із запропонованих стратегічних пріоритетів забезпечення кіберзахисту та зміцнення кібербезпеки вважаємо за доцільне відобразити на рис. 3.3.

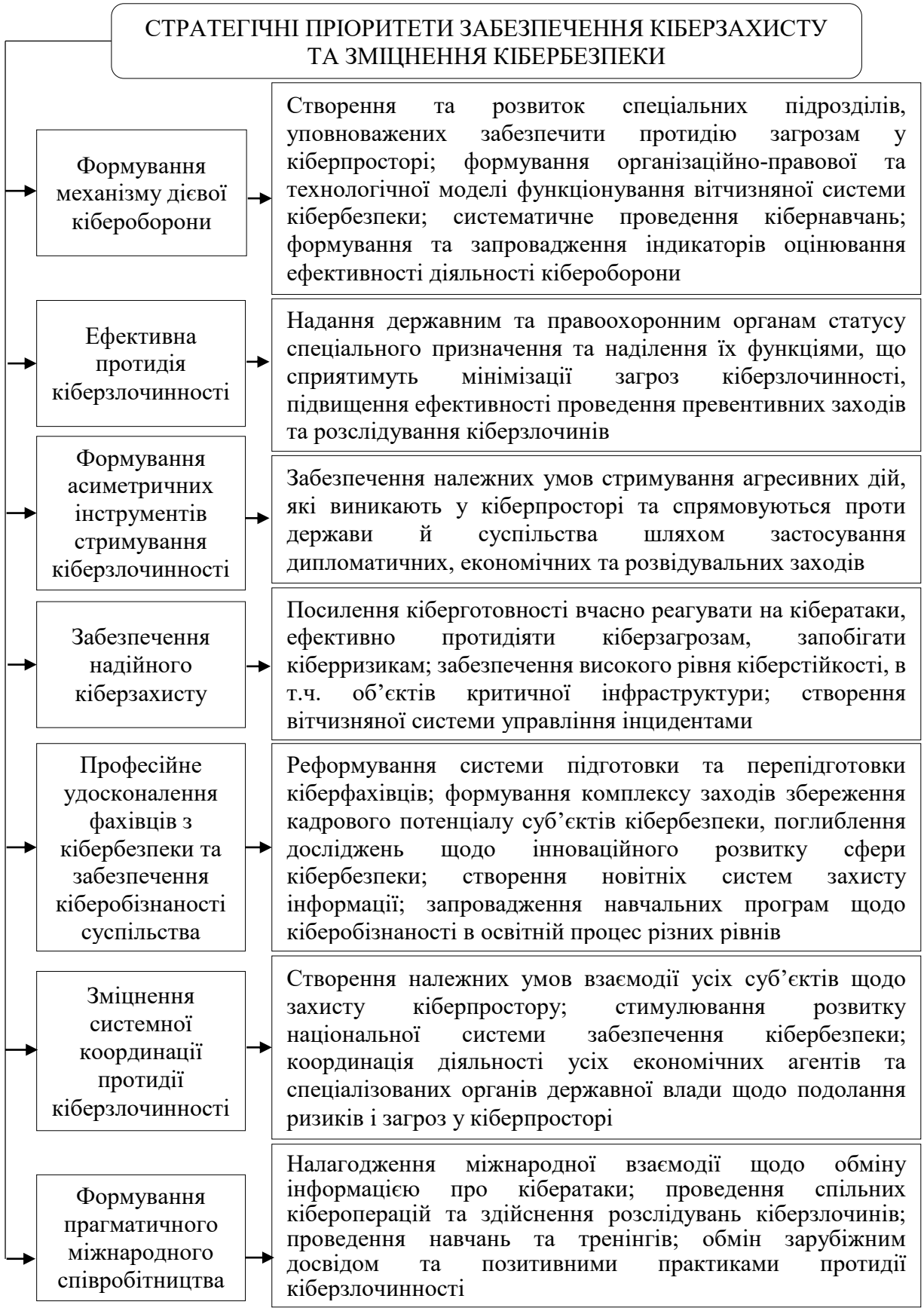


Рис. 3.3. Основні стратегічні пріоритети забезпечення кіберзахисту та зміцнення кібербезпеки в Україні

Джерело: складено автором за даними [49]

Очевидно, що окрім усього зазначеного, важливим завданням України у сфері протидії кіберзлочинності залишається поглиблення процесів євроінтеграції, що дозволить здійснити уніфікацію існуючих підходів до забезпечення кіберзахисту й кібербезпеки, а також сформувати перелік типових методів, способів та засобів вчинення кіберзлочинів та розробити комплекс заходів запобігання кіберризикам та кіберзагрозам. Важливою також є адаптація позитивних європейських та світових практик боротьби із кіберзлочинністю та взаємодії із зарубіжними партнерами.

Якісно новим завданням для вітчизняної системи протидії кіберзлочинності є запровадження та розвиток мультистейкхолдерської моделі управління інтернет-ресурсами, яка окремими авторами трактується як багатоформатна та різностороння. Проте, варто констатувати, що даний напрямок міжнародної взаємодії на сучасному етапі потребує поглибленого вивчення та проведення додаткових досліджень як зі сторони науковців, так і зі сторони провідних інститутів громадськості.

Таким чином, проведені дослідження національної системи протидії кіберзлочинності дозволили встановити необхідність її удосконалення. Виокремлено основні напрями протидії кіберзлочинності в Україні, а саме: зниження рівня технологічної залежності України від зарубіжних виробників інформаційно-комунікаційних технологій; удосконалення законодавчого забезпечення сфери кібербезпеки; посилення контролю за кіберзахистом та кіберграмотності фахівців і громадськості; формування нормативно-правових документів регулювання відносин щодо посилення кіберзахисту об’єктів критичної інфраструктури; формування системи забезпечення кібербезпеки держави та посилення захисту інформації, яка є з обмеженим доступом.

3.2. Досвід зарубіжних країн щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності

Транснаціональний характер поширення кіберзлочинності створює низку проблем, які становлять суттєву перешкоду реалізації заходів ефективної протидії даному деструктивному й загрозливому явищу. Активізація недобросовісної діяльності у кіберпросторі та вчинення протиправних діянь із використанням сучасних інформаційних технологій, які призводять до легалізації тіньових капіталів, дедалі частіше перебуває у центрі уваги світової спільноти, оскільки пошук ефективних методів протидії кіберзлочинності досі не увінчався успіхом. Стає очевидним, що проводити боротьбу із кіберзлочинністю на рівні однієї країни немає змісту, тому обґрунтованим виявляється налагодження дієвої міжнародної взаємодії в даному керунку.

Проведені нами дослідження основних тенденцій кіберзлочинності в Україні й зарубіжних країнах та здійснення оцінок обсягів легалізованих коштів, які акумульовані за допомогою кіберпростору, свідчать про неоднозначні позиції різних країн щодо боротьби із кіберзлочинністю. Встановлено, що високо розвинуті країни вживають більш ефективних заходів протидії злочинності у кіберпросторі, а країни, що розвиваються не спроможні забезпечити достатній рівень кібербезпеки та захистити фінансові операції у віртуальному середовищі, оскільки даний вид злочинності використовує глобальну мережу Інтернет, що допомагає зловмисникам охопити значні території для вчинення злочинів, а сліди таких злочинів усунути впродовж короткого періоду часу.

Крім того, значний ступінь анонімності вчинення кіберзлочинів не сприяє правоохоронній системі швидко реалізувати необхідні заходи щодо їх виявлення та розкриття. Зважаючи на окреслене, нагальною потребою сучасності являється налагодження ефективної системи міжнародного співробітництва та обміну досвідом протидії кіберзлочинності. Своєю чергою,

запозичення позитивного досвіду зарубіжних країн у сфері протидії легалізації злочинно отриманих коштів внаслідок діяльності кіберзлочинності є надзвичайно актуальним.

Варто зауважити, що лідируючі позиції щодо ефективності боротьби із кіберзлочинністю мають США, Великобританія та низка високо розвинутих країн Європейського Союзу, які спромоглися швидко прийняти національні стратегії безпеки в кіберпросторі та розробити комплекс заходів ефективної протидії. Зокрема, такий стратегічний документ США датований 2001 р., в Європейському Союзі Стратегія кібербезпеки ЄС [50] прийнята у 2013 р., а в Україні основний стратегічний документ, що регулює відносини у сфері протидії кіберзлочинності, прийнято лише у 2021 р. Очевидно, що регламентація таких важливих для боротьби із кіберзлочинністю документів не створила надійного підґрунтя для повного подолання даного деструктивного явища, про що свідчить наявність значних кіберзагроз та кіберризиків у сучасному суспільстві та посилення кіберзлочинності, особливо у період пандемії COVID-19, однак, позитивні зрушення таки зроблено.

Водночас, на міжнародному рівні потребують уніфікації певні дискусійні положення щодо функціонування глобальної системи кібербезпеки, серед найбільш вагомих із яких варто виділити:

1) несформованість єдиної європейської системи заходів реагування на кібератаки;

2) відмінність та багатоформатність національних стандартів боротьби з кіберзлочинністю та забезпечення кібербезпеки зарубіжних країн;

3) несформованість чіткого категоріального апарату у сфері кібербезпеки, який би уніфіковував основні підходи до дослідження даної проблематики;

4) функції боротьби із кіберзлочинністю, здебільшого, покладено на підрозділи поліції, а створення спеціальних підрозділів протидії кіберзлочинності не є загальнообов’язковим.

Не менш важливою залишається проблема формування моделі міжнародної системи забезпечення кібербезпеки, що, на думку О. Полякова [51, с. 130] здійснюється надто повільно та непередбачувано, а формування єдиного стратегічного курсу щодо боротьби із кіберзлочинністю має гібридний характер. Безумовно варто констатувати, що ефективна протидія кіберзлочинності та спробам легалізувати тіньові капітали із використанням кіберпростору неможливі без забезпечення достатнього рівня кібербезпеки як на міжнародному, так і на національному рівнях.

За таких умов актуалізується необхідність дослідження правового регулювання протидії кіберзлочинності, яке здійснюється різними країнами світу, та формування найбільш прийнятних для України моделей. Для деталізації основних наукових підходів пропонуємо виокремити особливості такого регулювання у країнах Європейського Союзу, адже, зважаючи на значні досягнення України на шляху до євроінтеграції та набуття нею статусу кандидата на вступ до ЄС, такий досвід є надзвичайно важливим.

Зазначимо, що правове регулювання системи протидії кіберзлочинності на теренах Європейського Союзу здійснюється за подвійними стандартами, зокрема:

1) у більшості країн ЄС наявна нормативно-правова база в частині протидії кіберзлочинності враховує норми національного та міжнародного права;

2) основні заходи, що спрямовані на протидію кіберзлочинності, здійснюються одночасно спеціалізованими організаціями національного та міжнародного рівнів;

3) належна увага приділяється міжвідомчій взаємодії, а активний інформаційний обмін проводиться з урахуванням інтересів зарубіжних країн;

4) на національному рівні стимулюються наукові розробки щодо проведення експертної оцінки кіберзлочинів, апробації методів їх виявлення, профілактика та підвищення ефективності розслідувань, однак, досі відсутня єдина система заходів щодо проведення таких експертиз.

Причому, в країнах Європейського Союзу значні зусилля спрямовуються на попередження та раннє виявлення кіберзлочинів на етапах здійснення кібератак та кіберінцидентів.

Варто зазначити, що на сучасному етапі Україна успішно адаптувала позитивний європейський досвід формування ситуаційних центрів кіберзахисту на об'єктах критичної інфраструктури, проте, імплементовані заходи не дозволяють в повній мірі забезпечити захист таких об'єктів, а їх постійні обстріли Російською Федерацією в ході російсько-української війни вимагають посилення захисних функцій.

Водночас, позитивною для України виявлено практику протидії кіберзлочинності у США, яка потребує уваги та визначення можливостей адаптації в умовах функціонування України. Позитивним явищем національної системи протидії кіберзлочинності США є жорстка відповідальність за вчинення протиправних діянь у кіберпросторі. Саме даний елемент найбільш вагомо відрізняє американську систему боротьби із кіберзлочинністю від європейської, де усталено правові норми, відповідно до яких кримінальні розслідування проводяться лише у випадках загрози національній безпеці країни та порушення інтересів держави й основних прав громадян.

Безумовно, протидія кіберзлочинності у США вважається одним із найважливіших пріоритетів державної політики, тому дана країна в умовах сучасності є найбільш захищеною від кібератак та від впливу кіберзагроз. Причому, США одні із перших сформували стандарти з безпеки у кіберпросторі, які сприяють швидкому виявленню, попередженню та протидії кіберзлочинам.

Позитивною практикою протидії кіберзлочинності у світовому масштабі варто назвати створення спеціальних підрозділів, які уповноважені здійснювати усі необхідні заходи запобігання, виявлення та протидії кіберзлочинам. Зокрема, достатньо розвинутими у даному питанні є США, Великобританія, Нідерланди, Австрія, Данія, Канада, Бельгія, Естонія,

Німеччина, Швеція, Норвегія, Швейцарія та Польща. Низький рівень розвитку й функціонування таких підрозділів зафіксовано в країнах транзитивного типу, незалежно від їх приналежності до конкретного регіонального об'єднання.

Значно підвищить ефективність вітчизняної системи протидії кіберзлочинності законодавче врегулювання проблемних питань одержання та передачі електронних доказів вчинення кіберзлочинів, що успішно реалізовано та апробовано у США, Великобританії та в країнах, що входять до Європейського Союзу. Необхідно зазначити, що такий механізм обміну кібердоказами широко враховує дестабілізуючий вплив викликів та небезпек сучасності. Проте, як на міжнародному, так і на національному рівні існує достатньо значна проблема, що пов'язана із відсутністю методики формування комплексної статистики щодо кіберзлочинності, внаслідок чого провести достовірні оцінки її обсягів стає неможливим.

Ще однією перешкодою протидії розвитку кіберзлочинності в Україні є відсутність законодавчих підстав для проведення віддалених обшуків інформаційних ресурсів, зокрема тих, що розміщені за межами території країни. В даному керунку варто запозичити позитивний досвід реалізації зазначеного, що присутній у Франції, де за допомогою укладення спеціальних угод скасовано державні кордони в питаннях протидії кіберзлочинності, що дозволяє країні:

1) здійснювати державне регулювання суспільних відносин в Інтернеті;

2) контролювати дії користувачів через формування та встановлення вимог обов'язкової авторизації розробників веб-сайтів;

3) налагодити злагоджену взаємодію правоохоронних органів із Інтернет-провайдерами в межах швидкого реагування та опрацювання загроз, що виникають у кіберпросторі.

Варто позитивно оцінити діяльність країн Європейського Союзу щодо протидії кіберзлочинності шляхом створення спеціальних комп'ютерних груп

реагування на надзвичайні ситуації, що виникають у кіберпросторі, які позиціонуються як CERT. Зауважимо, що такий підрозділ як CERT–UA вже успішно функціонує в Україні та здійснює систематизацію й аналітичні оцінки даних про кіберпреценденти, реєструє види кіберзлочинів, надає економічним агентам практичну допомогу щодо запобігання кіберризикамв та мінімізації наслідків впливу кібератак.

Водночас, потребують узагальнення основні напрямки запозичення позитивного міжнародного досвіду протидії кіберзлочинності та визначення шляхів його адаптації до умов функціонування національної системи протидії кіберзлочинності, які відобразимо на рис. 3.4.

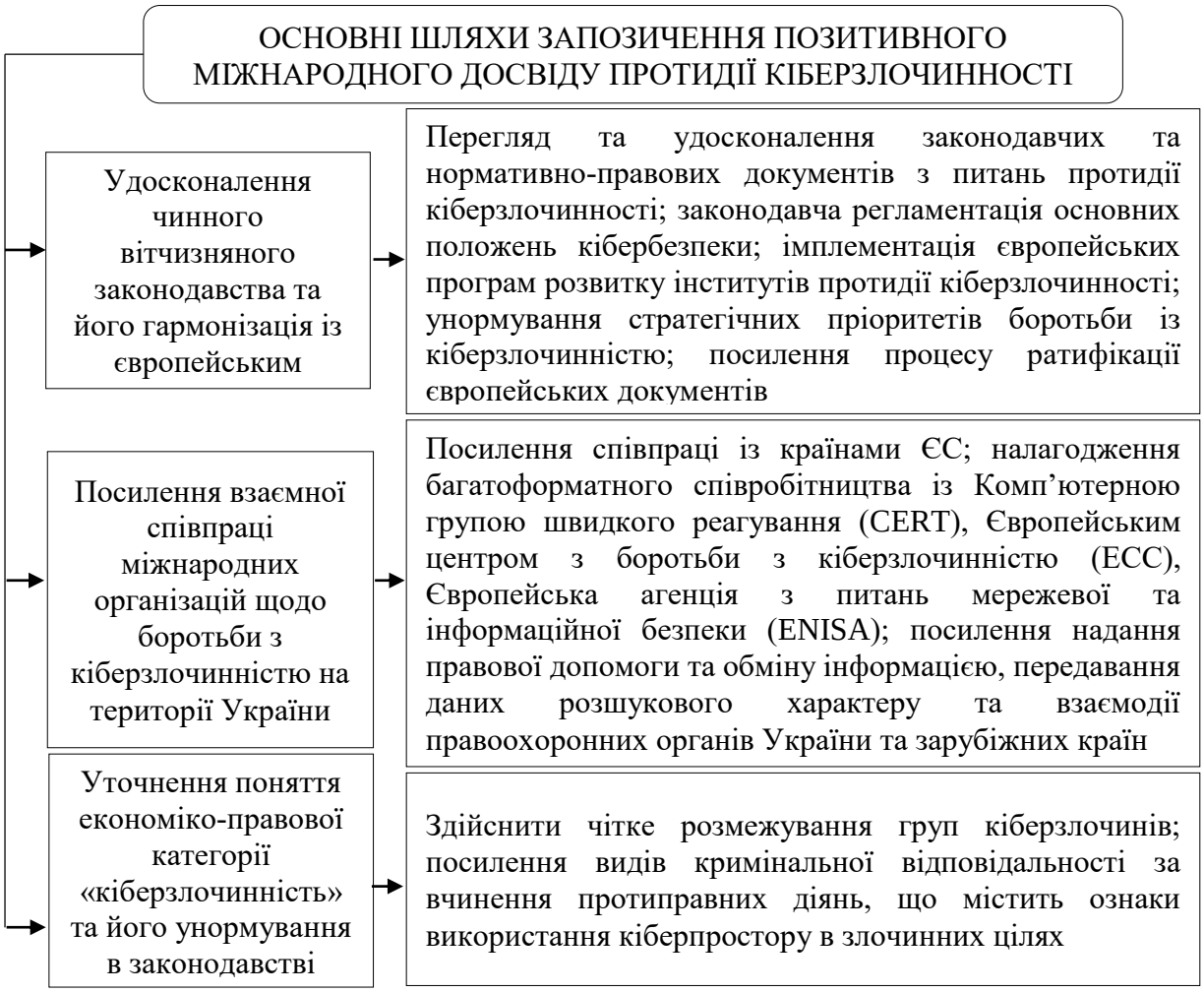


Рис. 3.4. Основні шляхи запозичення позитивного міжнародного досвіду протидії кіберзлочинності

Джерело: складено автором за даними [52, с. 42]

Варто відмітити вагомість діяльності міжнародних організацій у сфері боротьби із кіберзлочинністю, адже вони роблять значний внесок в глобальну систему попередження кіберзлочинності. Зокрема, Комп'ютерною групою швидкого реагування (Computer Emergency Response Team) проводиться формування системи спеціалізованих технологічних датчиків, за допомогою яких одержується можливість виявлення кібератак, а одержана інформація про можливі спроби вчинення кіберзлочинів передається Європейському центру з боротьби з кіберзлочинністю (European Cybercrime Centre), де систематизовується та аналізається інформація й спрямовується як підстава для організації спеціальних кібероперацій до Європейської агенції оборони (European Defence Agency) або до Європейської служби зовнішніх справ (European External Action Service). Поряд із цим, Європейська агенція з питань мережевої та інформаційної безпеки (European Union Agency for Cybersecurity) здійснює виявлення й блокування кібератак та усунення наслідків їх деструктивного впливу.

Комплексна реалізація заходів протидії кіберзлочинності на міжнародному рівні та тісна взаємодія із спеціалізованими міжнародними організаціями дозволить досягнути бажаного ефекту та знизити рівень вчинення кіберзлочинів.

Отже, проведені узагальнення досвіду зарубіжних країн щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності, дають підстави стверджувати, що найбільш розвинутою системою протидії кіберзлочинності є система США. Що стосується України, то вона частково запровадила позитивну практику протидії кіберзлочинності, яка сформована в країнах Європейського Союзу. Виявлено, що поглиблення потребує налагодження міжнародної взаємодії України у сфері боротьби із кіберзлочинністю та посилення співпраці із такими спеціалізованими міжнародними організаціями як Комп'ютерна група швидкого реагування, Європейський центр з боротьби з кіберзлочинністю, Європейська агенція оборони, Європейська служба зовнішніх справ та Європейська агенція з питань мережевої та інформаційної безпеки.

Висновки до розділу 3

Результати проведених досліджень стратегічних пріоритетів протидії легалізації доходів, отриманих у сфері кіберзлочинності, засвідчують необхідність удосконалення національної системи протидії кіберзлочинності, так як існуючі заходи боротьби з даним негативним явищем не дають бажаних результатів, а обсяги легалізованих коштів, отриманих у сфері кіберзлочинності продовжують зростати.

Доведено значну залежність та вразливість національної системи протидії кіберзлочинності від дестабілізуючого впливу внутрішніх та зовнішніх ризиків і загроз.

Визначено основні напрямки протидії кіберзлочинності в Україні, серед найвагоміших із яких є зниження зовнішньої технологічної залежності країни від виробників цифрових технологій, удосконалення законодавства у сфері кібербезпеки та формування її дієвої системи, посилення кіберзахисту, підвищення фаховості, кваліфікації та обізнаності у сфері кібербезпеки працівників спеціалізованих органів державної влади.

Окреслено стратегічні пріоритети забезпечення кіберзахисту та зміцнення кібербезпеки в Україні, до яких віднесено: формування механізму дієвої кібероборони, асиметричних інструментів стримування кіберзлочинності, забезпечення, прагматичного міжнародного співробітництва, зміцнення системної координації протидії кіберзлочинності, забезпечення надійного кіберзахисту та професійне удосконалення фахівців з кібербезпеки.

Дослідження досвіду зарубіжних країн щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності, доводить необхідність уніфікації основних засад функціонування глобальної системи кібербезпеки та потребу удосконалення правового регулювання системи протидії кіберзлочинності.

ВИСНОВКИ

Здійснивши ґрунтовні дослідження теоретико-прикладних засад протидії легалізації доходів, отриманих у сфері кіберзлочинності, оцінивши стан та тенденції протидії легалізації доходів, отриманих у сфері кіберзлочинності та систематизувавши стратегічні пріоритети протидії легалізації доходів, отриманих у сфері кіберзлочинності, нами проведено узагальнення наукових підходів до визначення сутності кіберзлочинності, її ролі в системі легалізації злочинно одержаних тіньових капіталів та значного негативного впливу на національну економіку й суспільство. На підставі одержаних результатів можна сформулювати наступні висновки:

1. Сутність легалізації доходів, отриманих злочинним шляхом, полягає у вчиненні спеціальних дій, спрямованих на узаконення та набуття вигляду одержаних в офіційному секторі економіки грошових коштів та активів, які спрямовуються для особистого збагачення та подальшого залучення в національну економіку. Легалізація доходів, отриманих злочинним шляхом, має значний деструктивний вплив на соціально-економічний розвиток країни та сприяє інтенсифікації розвитку кіберзлочинності.

2. Дослідження проблем стрімкого поширення кіберзлочинності дозволили з’ясувати, що вона характеризується як окремий вид кримінальної діяльності організованих злочинних груп та здійснюється з використанням кіберпростору. Основними мотивами вчинення кіберзлочинів є прагнення зловмисників до одержання неправомірної вигоди та отримання доступу до інформаційних ресурсів. В умовах сьогодення значного поширення набуває істотна різноманітність видів кіберзлочинів, які набувають транснаціонального масштабу, а наслідки поширення кіберзлочинності становлять значну загрозу державі та суспільству.

3. Здійснивши аналіз обсягів легалізації доходів, отриманих у сфері кіберзлочинності, в Україні встановлено зростаючі тенденції щодо активізації

кіберзлочинності. Виявлені обсяги легалізованих коштів із використанням кіберпростору досягнули 71,6 млн. грн. щорічно, а виникнення нових схем вчинення кіберзлочинів засвідчує потребу формування ефективної системи протидії кіберзлочинності.

4. Проведені оцінки динаміки кіберзлочинності в Україні дають підстави для висновку, що в країні спостерігається стрімке зростання кіберзлочинів, загальна кількість яких у 2021 р. досягнула позначки у 10020. Найбільша кількість кіберзлочинів впродовж 2017–2021 рр. зафіксована у банківській сфері. Зростаючі тенденції щодо кіберзлочинності потребують виважених заходів забезпечення кібербезпеки, Глобальний індекс якої свідчить про достатньо низький рівень кіберзахисту в Україні. Виявлено значні суми витрат, що спрямовуються країнами світу на забезпечення кібербезпеки та захисту інформації у кіберпросторі.

5. Запропоновано основні напрями удосконалення національної системи протидії кіберзлочинності, зокрема: зниження рівня технологічної залежності від іноземних виробників інформаційно-комунікаційних технологій; удосконалення нормативно-правової бази забезпечення кібербезпеки; посилення контрольних заходів щодо підвищення рівня кіберзахисту; проведення навчальних заходів, спрямованих на підвищення кіберграмотності фахівців і громадськості; формування спеціальних законодавчих документів, спрямованих на врегулювання відносин у сфері посилення кіберзахисту об’єктів критичної інфраструктури; забезпечення кібербезпеки держави та посилення захисту інформації з обмеженим доступом.

6. Узагальнення досвіду зарубіжних країн щодо протидії легалізації доходів, отриманих у сфері кіберзлочинності, дає можливість сформувати основні напрямки адаптації позитивних зарубіжних практик протидії кіберзлочинності до вітчизняних умов. Встановлено, що вагомого значення набуває уніфікація міжнародних та національних теоретико-прикладних засад функціонування глобальної системи кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Флейчук М.І. Легалізація економіки та протидія корупції у системі економічної безпеки: теоретичні основи та стратегічні пріоритети в умовах глобалізації: монографія. Львів: Ахілл, 2008. 660 с.

2. Білоус І.І. Сутнісна характеристика легалізації доходів, отриманих злочинним шляхом. *Економіка та держава*. 2019. № 5. С. 82–88.

3. Дудоров О.О., Тертиченко Т.М. Протидія відмиванню «брудного» майна: європейські стандарти та Кримінальний кодекс України: монографія. К.: Ваіте, 2015. 392 с.

4. Баранов Р.О. Сучасні схеми відмивання злочинних коштів у світі та в Україні. *Аспекти публічного управління*. 2015. № 7–8 (21–22). С. 62–69. URL: DOI: https://doi.org/10.15421/151559.

5. Рєзнік О.М., Щербак Н.М. Вплив легалізації доходів, одержаних злочинним шляхом, на фінансову систему України. Юридичний науковий електронний журнал. 2021. № 3. С. 290–293.

6. Лєонов С.В., Бойко А.О., Миненко С.В. Систематизація та характеристика існуючих схем легалізації доходів, отриманих незаконним шляхом. *Науковий вісник Полтавського університету економіки і торгівлі*. 2019. № 1 (92). С. 35–45.

7. Гончаренко І.Г. Аналіз ризику легалізації доходів, отриманих злочинним шляхом, через банки України. *Бізнесінформ*. 2019. № 9. С. 245–251.

8. Тарнавський Ю., Беседа Д., Момотенко Т., Суворов О., Каракасіді О. Протидія відмиванню доходів, одержаних злочинним шляхом: український та зарубіжний досвід. Журнал правових, етичних та регуляторних питань. 2020. Т. 23. Вип. 6. URL: https://www.abacademies.org/articles/combating-laundering-of-the-proceeds-from-crime-ukrainian-and-foreign-experience-9932.html.

9. Дубіняк Л. Боротьба з легалізацією (відмиванням) доходів, одержаних злочинним шляхом: удосконалення фінансового моніторингу.

Науковий блог Національного університету «Острозька академія». 2012. URL: https://naub.oa.edu.ua/2012/borotba-z-lehalizatsieyu-vidmyvannyam-dohodiv-oderzhanyh-zlochynnym-shlyahom-udoskonalennya-finansovoho-monitorynhu/.

10. Халін О.В. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом: монографія. Херсон ВД «Гельветика», 2018. 244 с.

11. Фролов С. Кримінально-правова та кримінологічна характеристика легалізації (відмивання) доходів, одержаних злочинним шляхом. *Юридичний вісник*. 2019. № 4. С. 130–136.

12. 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.

13. Підхомний О.М., Глущенка О.О. Аналіз чинників легалізації доходів, одержаних злочинним шляхом. *Фінансова система України*. 2008. Ч. 3. Вип. 10. С. 363–370.

14. Гула Л.Ф. Легалізація доходів, одержаних злочинним шляхом, що вчиняються організованими групами як одна з форм економічної загрози фінансовому ринку. Науковий вісник Львівського державного університету внутрішніх справ. 2014. Вип. 1. С. 331–342.

15. Лиман О.В., Мозгова М.В. Легалізація доходів, одержаних злочинним шляхом, через небанківські фінансові установи із залученням коштів та інших доходів громадян. Актуальні питання реформування правової системи України: матеріали міжнародної науково-практичної конференції (1–2 липня 2016 року). Дніпро: ГО «Правовий світ», 2016. С. 59–61.

16. Крайник Г.С., Заточна В.О. Проблемні питання кримінальної відповідальності за легалізацію (відмивання) доходів, одержаних у злочинний спосіб. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2019. Вип. 1 (85). С. 139–147.

17. Лєонов С., Бойко А., Боженко В., Лучко І. Роль та значення національної системи протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, у сучасних умовах розвитку фінансового ринку України. *Проблеми і перспективи економіки та управління*. 2018. № 3 (15). С. 137–144.

18. Аль-Махрукі А., Сіанаін К., Кечаді Т. Виклики кіберпростору та законодавчі обмеження. Міжнародний журнал передових комп'ютерних наук та застосувань. 2015. Т. 6. № 8. С. 279–289.

19. Valory G.E. Cyberspace and intelligence: Threats to intelligence, business and personal data will increase in 2022. *Modern Diplomacy*. 2022. URL: https://moderndiplomacy.eu/2022/03/01/cyberspace-and-intelligence-threats-to-intelligence-business-and-personal-data-will-increase-in-2022/.

20. Никончук Н.С., Маслова О.О. Кіберзлочинність в Україні: виклики сучасності. *Юридичний науковий електронний журнал*. 2021. № 9. С. 202–205.

21. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право.* 2019. № 1 (28). С. 108–117.

22. Germain J.M. The Future of Cybersecurity in 2021 and Beyond. URL: https://www.technewsworld.com/story/The-Future-of-Cybersecurity-in-2021-and-Beyond-87018.html.

23. 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.

24. Неділько Я. Поняття кіберзлочинів та їх види. Науковий часопис Національної академії прокуратури України. 2018. № 4. С. 49–60.

25. Бондаренком О.С., Рєпін Д.А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. С. 246–248.

26. Fischerkeller M.P. Current International Law is Not an Adequate Regime for Cyberspace. *LawFare, International Law*. URL:

https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace.

27. Конвенція про кіберзлочинність від 23.11.2001. № 994_575. Ратифікована 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

28. Сащенко М.І. Проблемні аспекти запобіггання кіберзлочинності в Україні. *Молодий вчений. Young Scientist.* 2022. № 1 (101). С. 17–20.

29. Кундеуса В.Г. Поняття та види кіберзлочинів. Держава і злочинність. Нові виклики в епоху постмодерну. 2020. С. 44–45. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/7723/Poniattia_Kundeus_2020.pdf?sequence=1&isAllowed=y.

30. Bargiacchi P. Cyberspace and International Law. International Workshop at Dokuz Eylul University. 2020. № 12. URL: https://www.academia.edu/44350226/CYBERSPACE_AND_INTERNATIONAL_LAW.

31. Звіт Державної служби фінансового моніторингу України за 2021 рік. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/zviti-pro-diyalnist/2021-rik/richnij-zvit-derzhfinmonitoringu-za-2021-rik.html

32. Академія фінансового моніторингу. Схеми: легалізація коштів від кіберзлочинів. URL: https://finmonitoring.in.ua/sxemi-nezakonne-spisannya-koshtiv-z-raxunkiv-z-distancijnim-keruvannyam/.

33. Звіт Державної служби фінансового моніторингу України за 2017 рік. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/zviti-pro-diyalnist/2017-rik/richnij-zvit-derzhfinmonitoringu-za-2017-rik.html

34. Звіт Державної служби фінансового моніторингу України за 2018 рік. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/zviti-pro-diyalnist/2018-rik/richnij-zvit-derzhfinmonitoringu-za-2018-rik.html

35. Звіт Державної служби фінансового моніторингу України за 2019 рік. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/zviti-pro-diyalnist/2019-rik/richnij-zvit-derzhfinmonitoringu-za-2019-rik.html

36. Звіт Державної служби фінансового моніторингу України за 2020 рік. URL: https://fiu.gov.ua/pages/dijalnist/funkcional/zviti-pro-diyalnist/2020-rik/richnij-zvit-derzhfinmonitoringu-za-2020-rik.html

37. Звіт Національної поліції України про результати роботи у 2017 р. URL: https://www.npu.gov.ua/diyalnist/zvitnist/richni-zviti.

38. Звіт Національної поліції України про результати роботи у 2018 р. URL: https://www.npu.gov.ua/diyalnist/zvitnist/richni-zviti.

39. Звіт Національної поліції України про результати роботи у 2019 р. URL: https://www.npu.gov.ua/diyalnist/zvitnist/richni-zviti.

40. Звіт Національної поліції України про результати роботи у 2020 р. URL: https://www.npu.gov.ua/diyalnist/zvitnist/richni-zviti.

41. Звіт Національної поліції України про результати роботи у 2021 р. URL: https://www.npu.gov.ua/diyalnist/zvitnist/richni-zviti.

42. Global Cybersecurity Index 2017. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

43. Global Cybersecurity Index 2018. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

44. Global Cybersecurity Index 2019. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/.

45. Global Cybersecurity Index 2020. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

46. Global Cybersecurity Index 2021. URL: https://www.itu.int/pub/D-STR-GCI.01-2021.

47. Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted. Statista. URL: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

48. Нікулеско Д. Кібербезпека: вразливі моменти. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html.

49. Про Рішення ради національної безпеки та оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента

України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n5.

50. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels 7.02.2013. URL: https://www.enisa.europa.eu/.

51. Поляков О.М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.

52. Buyadzha S. Positive experience of legal regulation of combating cybercrime in EU countries. *European Political and Law Discourse*. 2017. Vol. 4. Issue 4. C. 41–46.