DOI: https://doi.org/10.32782/2308-1988/2024-50-59
УДК 336.7:343.9

Боженко Вікторія Володимирівна
кандидат економічних наук, доцент,
доцент кафедри економічної кібернетики,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-9435-0065

Пахненко Олена Михайлівна
кандидат економічних наук, доцент,
доцент кафедри фінансових технологій і підприємництва,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-4703-4078

Койбічук Віталія Василівна
кандидат економічних наук, доцент,
завідувач кафедри економічної кібернетики,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-3540-7922

Яровенко Ганна Миколаївна
доктор економічних наук, доцент,
доцент кафедри економічної кібернетики,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-8760-6835

Victoria Bozhenko, Olena Pakhnenko, Vitalia Koybichuk, Ganna Yarovenko
Sumy State University

РОЗСЛІДУВАННЯ ФІНАНСОВИХ КІБЕРЗЛОЧИНІВ ТА ЦИФРОВА КРИМІНАЛІСТИКА У ФІНАНСОВІЙ СИСТЕМІ ЄС[1]

FINANCIAL CYBERCRIME INVESTIGATIONS AND DIGITAL FORENSICS IN EU FINANCIAL SYSTEM

Анотація. Стаття присвячена актуальним питанням цифрової криміналістики у фінансовій сфері з урахуванням досвіду ЄС. Авторами узагальнено результати наукових досліджень щодо формування портрету кіберзлочинця, проведена класифікація їх типів, а також надана порівняльна характеристика мотивів та особливостей злочинів, що вчиняються в офлайн та онлайн середовищі. В статті розглянуто динаміку кіберінцидентів, що відбуваються у фінансовій сфері, та виявлено суттєвий їх приріст за останні роки. Авторами узагальнено основні етапи цифрової криміналістики та ідентифіковано основні труднощі, з якими стикаються при розслідуванні кіберінцидентів у сфері фінансових послуг. Для подолання перешкод у цифровій криміналістиці у фінансовій сфері запропоновано поєднання передових інструментів судової експертизи, спеціалізованого досвіду та тісної співпраці між фінансовими установами, правоохоронними та регуляторними органами.

Ключові слова: кіберзлочин, цифрова криміналістика, портрет кіберзлочинця, фінансова система, фінансові кіберзлочини.

Summary. The article is devoted to current issues of digital forensics in the financial sphere, considering the experience of the European Union. The authors summarized the results of scientific research on the portrait of a cybercriminal, classified their types, and provided a comparative description of the motives and features of crimes committed offline and online. The motives of cybercriminals, which distinguish them from traditional criminals, are curiosity and challenge. In addition, a significant factor in the commission of crimes in cyberspace is anonymity, which reduces the risk of being exposed and increases the determination of cybercriminals. Depending on the motivation for hacking computer systems, white hat, grey hat and black hat hackers are distinguished. In addition to these main types, there are many other varieties: red hat, blue hat hackers, script kiddies, hacktivists and others. The

[1] Роботу виконано в рамках проєкту Жан Моне (Модуль) «Практики ЄС щодо захисту фінансової системи від кіберзагроз» (EU_PITCH).

article examines the dynamics of cyber incidents occurring in the financial sphere and reveals a significant increase in them for the period of 2021-2024. The authors specified the content of the main stages of digital forensics in terms of the following components: preparatory stage; identification of cyber threats; incident response; collection and preservation of digital evidence; investigation and analysis of digital evidence; cyber incident reporting; recovery from a cyber incident. The article identifies the main difficulties in the investigation of cyber incidents in the field of financial services. These include: integrated management system of financial institutions; encryption and secure communication channels that are inaccessible to forensic investigators; difficulties in tracking the source of illegal actions; regulatory and jurisdictional barriers; a significant amount of financial transactions; problems with cloud computing and virtualized environments; internal threats (breach of confidentiality by employees or contractors); limited resources and experience; the rapidly evolving threat landscape (constant adaptation and new methods of cybercrime in the financial sector). To overcome obstacles in digital forensics in the financial sector, a combination of advanced forensic tools, specialized expertise and close cooperation between financial institutions, law enforcement and regulatory authorities is proposed.

Keywords: cybercrime, digital forensics, portrait of a cybercriminal, financial system, financial cybercrimes.

Постановка проблеми. З розвитком цифрових технологій і фінансових інструментів спостерігається зростання випадків кіберзлочинності, таких як крадіжка особистих даних, фальсифікація транзакцій, фішинг, атаки на фінансові інститути тощо. Це створює серйозні загрози для стабільності функціонування фінансових систем і довіри до них, а також має негативні економічні наслідки, включаючи великі фінансові втрати для компаній і приватних осіб. Розвиток нових технологій, таких як блокчейн і штучний інтелект, з одного боку, відкриває можливості для покращення захисту фінансових даних і раннього виявлення кіберзагроз. З іншого боку, ці ж технології можуть використовуватися кіберзлочинцями для вдосконалення їхніх методів і інструментів, що змінює способи здійснення кіберзлочинів.

Відбуваючись в онлайн просторі, кіберзлочини часто носять міжнародний характер, що ускладнює їх розслідування через юрисдикційні питання та необхідність координації між різними країнами та правоохоронними органами. Отже, розслідування фінансових кіберзлочинів вимагає постійного оновлення знань і методик, а також міжнаціональної координації зусиль для ефективного протистояння цим загрозам, що робить питання цифрової криміналістики у фінансовій системі надзвичайно актуальними. Тоді як розуміння психологічних аспектів поведінки фінансових кіберзлочинців допомагає у вдосконаленні заходів з безпеки та захисту інформації.

Аналіз останніх досліджень і публікацій. Вивчення і запобігання фінансовій кіберзлочинності знаходиться на перетині економіки (питання фінансової безпеки, захисту платіжних систем тощо, фінансової грамотності і платіжної безпеки користувачів фінансових послуг тощо), комп'ютерних наук (технологічні аспекти забезпечення захисту даних, комп'ютерних мереж і систем), юридичних наук (цифрова криміналістика та правова відповідальність за кіберзлочини), психології і соціології (психологічний портрет кіберзлочинців, соціальна інженерія). Різними аспектами дослідження фінансових кіберзлочинів та цифрової криміналістики займаються вітчизняні та зарубіжні науковці, серед яких: Бабенко О.О., Мокляк А.С. [1], Коваль О.Є. [2], Світличний В.А. [3], Дзюндзюк В.Б., Кравцова М.О., Noordegraaf J.E. [4], Weulen Kranenbarg M. [4; 5], Leukfeldt E. [6], Richet J.-L. [7], Kerstens J., Jansen J. [8] та інші.

Отже, проблематика фінансової кіберзлочинності є складною і комплексною, а здатність кіберзлочинців нанести великих фінансових збитків на значної шкоди фінансовій безпеці як окремих осіб, установ, так і держави в цілому, робить її важливим фокусом досліджень як на національному рівні, так і в міжнародній площині. В Європейському Союзі функціонують спеціалізовані організації, які забезпечують протидію кіберзлочинам, проводять технічну експертизу з цих питань, моніторинг і підтримку нормативно-правового забезпечення (наприклад, підрозділ Європолу The European Cybercrime Centre – EC3, Агентство ЄС із питань кібербезпеки – ENISA), а також впроваджені в дію директиви з мережевої та інформаційної безпеки (NIS 2, 2023).

Метою статті є узагальнення результатів наукових досліджень щодо формування портрету кіберзлочинця та встановлення особливостей цифрової криміналістики у фінансовій сфері.

Виклад основного матеріалу дослідження. Одним із засобів контролю, які розробляють і впроваджують фінансові установи, є цифрова криміналістика, яка передбачає відновлення та дослідження інформації чи даних, пов'язаних із інцидентами чи підозрами в кіберзлочині, виявлених або збережених у системі базових програм фінансової установи чи на електронних чи цифрових пристроях. Цифрова криміналістика у фінансовому секторі передбачає застосування криміналістичних методів для аналізу фінансових правопорушень, таких як шахрайство, інсайдерська торгівля, відмивання грошей і розкрадання. Цифрова криміналістика спрямована на ідентифікацію, збір, аналіз та представлення цифрових доказів, які можна використовувати в суді або для внутрішніх розслідувань.

Важливим напрямком цифрової криміналістики і боротьби з кібершахрайствами є встановлення портрету кіберзлочинця і патернів його поведінки, а також ключових мотивів кіберзлочинів, з метою легшої і швидшої ідентифікації можливих загроз на основі виявлення факторів ризику та більш ефективної протидії злочинам у кіберпросторі. Узагальнення наукових досліджень з тематики мислення і поведінки кіберзлочинців [1, 2, 5, 9] засвідчує, що типовий портрет кіберзлочинця не є однозначно визначеним. В більшості випадків кіберзлочинцями є чоловіки середнього віку (30-40 років). За рештою ж психологічних, соціальних і особистісних характеристик кіберзлочинці можуть значно відрізнятися один від одного, що також залежить і від конкретного виду кіберзлочину, що ними вчиняється.

Серед основних рис, які вирізняють кіберзлочинців, найчастіше виокремлюють високий рівень їх технічних навичок, часто освіту або поглиблені знання у сфері ІТ; аналітичний склад розуму та допитливість; терпіння та володіння собою, адже злам комп'ютерних системи потребує багато часу і витримки; потреба долати труднощі, вирішувати головоломки. Серед негативних якостей таких людей найчастіше говорять про низьку комунікабельність, замкненість, схильність до ризику, маніпулятивність або навіть соціопатичні риси. Втім варто зауважити, що у фінансовій сфері кіберзлочинці частіше діють як організована група [6], а не окремі особистості. Найчастіше такі групи налічують близько 6 осіб, серед яких є як технічні фахівці з вищеназваними типовими рисами, так і інші типажі кіберзлочинців з іншими ролями («бос», «мислитель», «бухгалтер» тощо).

Для здійснення кіберзлочинів зловмисники часто використовують соціальну інженерію. Особливо яскраво це проявляється у кібершахрайствах у фінансовій сфері. Зловмисники намагаються створити атмосферу довіри, видаючи себе за надійну установу або особу, щоб отримати необхідну особисту інформацію від жертви для доступу до цільової мережі шляхом обману та маніпуляцій. Кібершахраї часто спрямовують свою діяльність на користувачів фінансових послуг, особливо представників вразливих груп населення. Вони використовують такі психологічні риси людей як бажання допомагати іншим, схильність довіряти, складність відмовляти, бажання чути лестощі тощо. Для впливу на людей кіберзлочинці активно використовують принципи соціальної інженерії, зокрема: авторитет (видають себе за авторитетних осіб або представників авторитетних організацій, щоб здобути довіру жертви); привабливість (можуть створювати ситуації або пропозиції, що здаються надзвичайно вигідними або привабливими, щоб спонукати жертву до дій); терміновість та дефіцит (використовують тактику терміновості або вдаються до створення ілюзії дефіциту, щоб змусити жертву діяти швидко без ретельного розгляду); сталість та послідовність (можуть вдаватися до техніки поступового переконання, де спочатку просять про незначні послуги, а з часом переходять до більш серйозних запитів); соціальний доказ (використовують соціальний доказ, стверджуючи, що інші люди вже виконали певні дії або прийняли певні рішення, щоб підштовхнути жертву до того ж); взаємність (пропонують безкоштовні послуги або інформацію, щоб викликати у жертви почуття обов'язку відповісти тим же) [3]. Оскільки більшість концепцій соціальної інженерії походить із психології, цим методам кіберзлочинців важко запобігти використовуючи чисто технічні, комп'ютерні засоби захисту. Серед основних напрямків мінімізації цього виду кіберзлочинів має бути просвітницька діяльність з платіжної безпеки і інформаційної безпеки в цілому.

Марлен Вейлен Краненбарг (Marleen Weulen Kranenbarg), яка понад 10 років займається цифровою криміналістикою, у своїх дослідженнях виділяє шість основних мотивів здійснення кіберзлочинів: цікавість, виклик (челендж), гнів, помста, хіть (бажання) і жадібність [4, 5, 9]. В цілому ці мотиви є спільними як для офлайн, так і онлайн злочинців, втім цікавість і виклик часто є ключовими мотивами для більшості хакерів, які перевіряють свою здатність проникнути в комп'ютерну мережу, не ставлячи першочергову мету отримання фінансової вигоди чи завдання шкоди. Значною мірою їх тягне до подолання труднощів: чим складніша система, тим привабливіша вона для хакера [2]. Ключовим фактором, що посилює ймовірність здійснення особою злочину у кіберпросторі є анонімність. Можливість приховати свою особистість і місцезнаходження та не бути викритим приваблює багатьох злочинців і робить їх сміливішими.

Слід зауважити, що поняття «хакер» увійшло в обіг і стало популярним для позначення злочинців у кіберпросторі, однак початково це поняття не носило негативного криміналістичного відтінку. Натомість, поняття крекер («cracker» або зломщик) позначає особу, яка здійснює злам системи з метою нанесення шкоди. Звуження загальновживаної термінології на позначення зловмисників у кіберпросторі до поняття «хакер», призвело до необхідності проведення їх класифікації за основними мотивами та напрямками зловмисної діяльності. Основна класифікація передбачає виокремлення чорних, білих та сірих хакерів. Білі або етичні хакери цілком працюють в легальному просторі, є фахівцями з комп'ютерної безпеки та здійснюють перевірку систем на можливість зламу на замовлення певної компанії. В багатьох

країнах, у тому числі в ЄС, проводиться навчання та сертифікація етичних хакерів.

Чорні хакери становлять найбільшу загрозу, адже їх мета отримати несанкціонований доступ до комп'ютерних систем, зламати систему даних або отримати фінансову вигоду. Сірі хакери можуть не мати злочинних намірів, коли шукають слабкі місця в безпеці програмного забезпечення, однак діють без згоди чи попередження компанії. Крім основної класифікації на білих, сірих і чорних хакерів виділяють інші підтипи, такі як зелені хакери (малодосвідчені), червоні хакери (спрямовують свою діяльність проти чорних хакерів), хактивісти (використовують хакерство для того, щоб донести певне політичне, релігійне чи соціальне повідомлення) та інші.

Кількість кіберзлочинців продовжує неухильно зростати як завдяки новим технологіям, які полегшують доступ до злочинної діяльності, так і завдяки зростанню складності цифрової інфраструктури, яка розширює потенційний простір для атаки [10]. Обсяг значущих кіберінцидентів, прямо чи опосередковано пов'язаних з діяльність фінансових установ, також перманентно зростає. Протягом 2011-2024 років у світі відбулося 2504 кіберінцидентів, які мали суттєвий вплив на функціонування фінансового сектору економіки або призвели до значних фінансових та репутаційних збитків (European Repository of Cyber Incidents, EuRepoC) (рис. 1) [11]. Майже 20% кіберінцидентів були реалізовані з використанням програм-здирників, після чого відбувається дешифрування даних.

Зростання кількості кіберіндидентів вимагає посиленої уваги регуляторних органів до питань кібербезпеки, особливо у фінансовій сфері. Фінансовий сектор підпадає під дію суворої нормативно-правової бази у сфері кібербезпеки, що передбачає дотримання єдиних вимог та рекомендацій у сфері управління кіберризиками фінансових установ в країнах ЄС.

Одним із ключових напрямків в системі протидії кіберзагрозам у сфері фінансових послуг є удосконалення процедури цифрової криміналістики та звітування й розкриття фінансовими установами про кіберінциденти. У таблиці 1 представлено основні етапи цифрового розсліджування кіберзлочинів у сфері фінансових послуг.

Кіберзлочинці використовують технологічно складні та добре замасковані методи атак на комп'ютерні системи та мережі, і тому для успішного розслідування таких випадків необхідно мати високий рівень технічної експертизи та доступ до передових інструментів цифрової криміналістики. Основними труднощами при розслідуванні кіберінцидентів у сфері фінансових послуг є:

1. Інтегрована система управління. Фінансові установи використовують складні операційні системи та обробляють величезні обсяги фінансових даних. Ці системи зазвичай інтегровані в декілька платформ, включаючи банківське програмне забезпечення, торгові платформи та системи бухгалтерського обліку. Складність і взаємозв'язок ускладнюють відстеження та аналіз конкретних фінансових операцій, особливо коли кіберзлочинці маніпулюють даними або приховують їх.

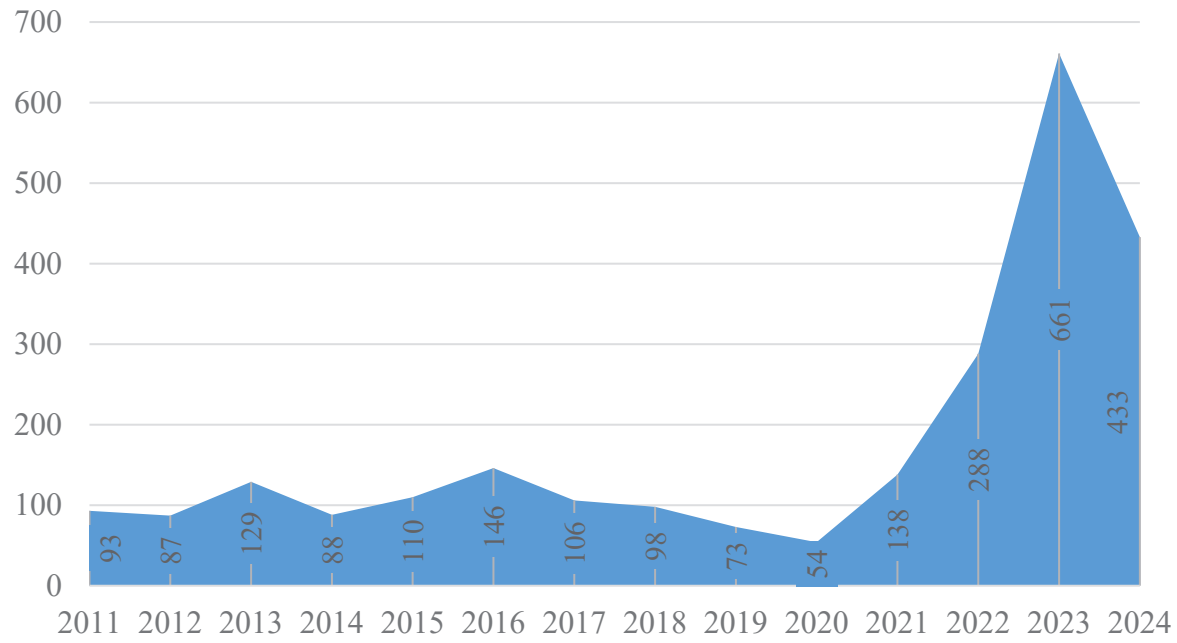

Рисунок 1 – Динаміка значущих кіберінцидентів у фінансовій сфері

Джерело: дані Європейського репозитарію кіберінцидентів [11]

Таблиця 1 – Основні етапи цифрової криміналістики

Етапи	Зміст етапу
Підготовчий етап	– впровадження заходів кібербезпеки (шифрування, надійна автентифікація та системи моніторингу, брандмауери, системи виявлення вторгнень); – створення плану реагування на інцидент; – навчання співробітників щодо обізнаності з кібербезпеки та їхніх ролей у реагуванні на інциденти; – налаштування цифрових криміналістичних інструментів для збору, аналізу та збереження даних
Ідентифікація кіберзагроз	– виявлення аномалій або підозрілих дій, які можуть свідчити про порушення безпеки; – впровадження автоматичних сповіщень про аномалії (наприклад, великі неавторизовані транзакції, доступ до конфіденційних даних). – попередній аналіз аномалій або інциденту, щоб визначити його характер і потенційний вплив на фінансову установу та її стейкхолдерів;
Реагування на інциденти	– повідомлення ключових зацікавлених сторін і групи реагування на інциденти; – ініціювання процедур стримування для запобігання поширенню інциденту (блокування відповідних банківських рахунків, захист скомпрометованих систем, відключення уражених мереж або систем від решти інфраструктури.
Збір та збереження цифрових доказів	– отримання цифрових доказів з різноманітних джерел та інструментів; – зберігання доказів у безпечному середовищі з контрольованим доступом.
Розслідування та аналіз цифрових доказів	– перевірка файлових систем, записів електронної пошти та мережевого трафіку на наявність ознак зловмисної діяльності; – відновлення хронології інциденту; – виявлення векторів нападу та методів, які використовували зловмисники.
Звітування про кіберінцидент	– складання детальних звітів про кіберінцидент у визначені строки – повідомлення постраждалих сторін, наприклад клієнтів, якщо особисті дані були скомпрометовані. – у деяких випадках цифрові докази можуть бути використані в судовому процесі для переслідування кіберзлочинців
Відновлення після кіберінциденту	– оновлення планів реагування на інциденти, політики та програм навчання. – застосування додаткових засобів контролю або інструментів, необхідних для усунення прогалин, виявлених під час інциденту.

Джерело: складено авторами на основі [12-16]

2. Шифрування та безпечні канали зв'язку. У фінансовому секторі надійне шифрування широко використовується для захисту конфіденційних даних, таких як інформація про клієнтів, деталі транзакцій і зв'язок між системами. Незважаючи на те, що шифрування має важливе значення для безпеки, шифрування створює серйозну проблему для судових слідчих, яким потрібно отримати доступ і проаналізувати ці дані без ключів дешифрування, які часто недоступні через суворі протоколи безпеки.

3. Відстеження джерела незаконних дій. Розслідування проводиться для виявлення інформації про кіберзлочин, які попередньо можуть бути видалені або скомпроментовані кіберзлочинцями. Кіберзлочинці можуть використовувати наступні методи: обфускація даних, безпечне видалення файлів, стеганографія для приховування незаконних транзакцій або комунікацій.

4. Регуляторні та юрисдикційні перешкоди. Фінансові злочини часто стосуються кількох юрисдикцій, особливо коли трансакції перетинають міжнародні кордони. Відмінності в нормативних базах, законах про конфіденційність і фінансових правилах можуть створювати перешкоди для отримання та обміну цифровими доказами. Судові слідчі повинні орієнтуватися в складних правових умовах, щоб зібрати докази, прийнятні в суді, що може затримати або ускладнити розслідування.

5. Значний обсяг фінансових операцій. Фінансовий сектор щодня генерує величезний обсяг транзакцій, кожна з яких має кілька точок даних. Фільтрування цих даних для виявлення підозрілих дій або шахрайських транзакцій займає багато часу та ресурсів. Величезний обсяг може перевантажити криміналістичні інструменти та аналітиків, ускладнюючи ідентифікацію та виділення критичних доказів.

6. Проблеми з хмарними обчисленнями та віртуалізованими середовищами. Значна кількість фінансових установ використовують хмарні служби та віртуалізоване середовище для управління даними. Це створює проблеми для цифрової криміналістики, оскільки дані можуть бути розподілені в кількох місцях, що ускладнює визначення місця зберігання конкретних доказів. Крім того, отримання доступу до даних, що зберігаються в хмарі, часто вимагає співпраці з постачальниками хмарних послуг, які можуть

мати суворий контроль доступу та політику конфіденційності.

7. Внутрішні загрози. Співробітники або підрядники, які мають доступ до конфіденційних систем і даних, можуть зловживати своїми правами для вчинення шахрайства чи інших кіберзлочинів. Для виявлення та розслідування інсайдерської діяльності потрібні складні криміналістичні інструменти, які можуть відстежувати та аналізувати поведінку користувачів, не порушуючи норм конфіденційності.

8. Обмеження ресурсів і досвіду. Цифрова криміналістика у фінансовому секторі потребує спеціальних знань та інструментів, які можуть бути дорогими та ресурсомісткими. Не всі фінансові установи мають можливість утримувати спеціальну групу експертів, що призводить до покладання на зовнішніх експертів, що може затримати процес розслідування та збільшити витрати.

9. Ландшафт загроз, що швидко розвивається. Кіберзлочинці постійно адаптують і розробляють нові методи використання вразливостей у фінансовому секторі. Швидка еволюція загроз означає, що судові слідчі повинні постійно оновлювати свої знання та інструменти, щоб не відставати. Ця постійна проблема ускладнює випередження кіберзлочинців і ефективне розслідування фінансових кіберзлочинів.

Отже, фінансовий сектор стикається з унікальними та значними перешкодами в цифровій криміналістиці через складність фінансових систем, використання шифрування, нормативні проблеми та великий обсяг транзакцій. Щоб подолати ці перешкоди, потрібне поєднання передових інструментів судової експертизи, спеціалізованого досвіду та тісної співпраці між фінансовими установами, правоохоронними та регуляторними органами.

Висновки. Цифрова криміналістика є незамінною у фінансовому секторі, оскільки вона надає засоби для виявлення, розслідування та запобігання фінансовим злочинам, забезпечує дотримання нормативних вимог і захищає цілісність і репутацію фінансових установ. У міру того, як фінансові злочини стають все більш витонченими, роль цифрової криміналістики буде тільки зростати, роблячи її критичним компонентом фінансової безпеки та управління.

Список використаних джерел:

1. Бабенко О.О., Мокляк А.С. Теоретичний аналіз дослідження психологічного портрета кіберзлочинця. *Теорія і практика сучасної психології.* 2018. № 2. С. 89–93.

2. Коваль О.Є. Психологічний портрет кіберзлочинця. *Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід*: матеріали ІІ Міжнародної науково-практичної конференції (м. Тернопіль, 21-22 квіт. 2017р.). С. 189–192.

3. Світличний В.А. Деякі концепції соціальної інженерії. *Протидія кіберзлочинності та торгівлі людьми*: збірник матеріалів міжнародної науково-практичної конференції (м. Вінниця, 31 трав. 2023 р.). Вінниця: ХНУВС, 2023. С. 161–164.

4. Noordegraaf J.E., Weulen Kranenbarg M. Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. *Criminology & Public Policy*. 2023. Vol. 22. P. 803–824. DOI: https://doi.org/10.1111/1745-9133.12650

5. Weulen Kranenbarg M., van Gelder J.-L., Barends A. J., de Vries R. E. Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in Human Behavior*. 2023. Vol. 140. DOI: https://doi.org/10.1016/j.chb.2022.107576

6. Leukfeldt E., Lavorgna A., Kleemans E.R. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research.* 2017. Vol. 23. P. 287–300. DOI: https://doi.org/10.1007/s10610-016-9332-z

7. Richet J.-L. How cybercriminal communities grow and change: An investigation of ad-fraud communities. *Technological Forecasting and Social Change*. 2022. Vol. 174. DOI: https://doi.org/10.1016/j.techfore.2021.121282

8. Kerstens J., Jansen J. The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior.* 2016. Vol. 37(5). P. 585–600. DOI: https://doi.org/10.1080/01639625.2015.1060796

9. Inside the mind of a cybercriminal. BBVA Group. URL: https://www.bbva.com/en/innovation/inside-the-mind-of-a-cybercriminal/ (дата звернення: 12.08.2024).

10. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union, Luxembourg, 2024. DOI: https://doi.org/10.2813/442713

11. EuRepoc Data. European Repository of Cyber Incidents. URL: https://eurepoc.eu/databases (дата звернення: 25.08.2024).

12. Dzomira S. Digital forensic technologies as e-fraud risk mitigation tools in the banking industry: Evidence from Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions.* 2014. Vol. 4 (2-1). P. 116–124. DOI: https://doi.org/10.22495/rgcv4i2c1art4

13. Prasanthi B.V., Kanakam P., Hussain S.M. Cyber Forensic Science to Diagnose Digital Crimes- A study. *International Journal of Computer Trends and Technology*. 2017. Vol. 50(2). P. 107–113. DOI: https://doi.org/10.14445/22312803/ijctt-v50p119

14. Singh S., Kumar S. Qualitative Assessment of Digital Forensic Tools. *Asian Journal of Electrical Sciences*. 2020. Vol. 9(1). P. 25–32. DOI: https://doi.org/10.51983/ajes-2020.9.1.2372

15. Singh S., Singh V.K. Digital Forensic Investigation: Ontology, Methodology, and Technological Advancement. In Advancements in Cybercrime Investigation and Digital Forensics. Apple Academic Press, 2023. P. 137–160. DOI: https://doi.org/10.1201/9781003369479-7

16. Benjamine B. C., Subramaniam S. Enhancing the Financial Sector's Cyber Security in the Digital Economy. *Financial Stability Review.* 2019. P. 44–46. URL: https://www.bnm.gov.my/documents/20124/6433062/fsr2019h1_en_box2.pdf (дата звернення: 25.08.2024).

References:

1. Babenko O. O., Moklyak A. S. (2018) Teoretychnyy analiz doslidzhennya psykholohichnoho portreta kiberzlochyntsya [Theoretical analysis of the study of the psychological portrait of a cybercriminal]. *Teoriya i praktyka suchasnoyi psykholohiyi*, no. 2, pp. 89–93. (in Ukrainian)

2. Koval O. E. (April 21-22, 2017) Psykholohichnyy portret kiberzlochyntsya [Psychological portrait of a cybercriminal]. Ukrayina v umovakh reformuvannya pravovoyi systemy: suchasni realiyi ta mizhnarodnyy dosvid: materialy II Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi. Ternopil. Pp. 189–192. (in Ukrainian)

3. Svitlychny V. A. (May 31, 2023) Deyaki kontseptsiyi sotsialnoyi inzheneriyi [Some concepts of social engineering]. Protydiya kiberzlochynnosti ta torhivli lyudmy: zbirnyk materialiv mizhnarodnoyi naukovo-praktychnoyi konferentsiyi. Vinnytsya: KHNUVS, pp. 161–164. (in Ukrainian)

4. Noordegraaf J. E., Weulen Kranenbarg M. (2023) Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. *Criminology & Public Policy*, no. 22, pp. 803–824. DOI: https://doi.org/10.1111/1745-9133.12650

5. Weulen Kranenbarg M., van Gelder J.-L., Barends A. J., de Vries R. E. (2023) Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in Human Behavior*, no. 140. DOI: https://doi.org/10.1016/j.chb.2022.107576

6. Leukfeldt E., Lavorgna A., Kleemans E. R. (2017) Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research,* no. 23, pp. 287–300. DOI: https://doi.org/10.1007/s10610-016-9332-z

7. Richet J.-L. (2022) How cybercriminal communities grow and change: An investigation of ad-fraud communities. *Technological Forecasting and Social Change*, vol. 174. DOI: https://doi.org/10.1016/j.techfore.2021.121282

8. Kerstens J., Jansen J. (2016) The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior*, vol. 37(5), pp. 585–600. DOI: https://doi.org/10.1080/01639625.2015.1060796

9. Inside the mind of a cybercriminal. BBVA Group. Available at: https://www.bbva.com/en/innovation/inside-the-mind-of-a-cybercriminal/

10. Europol (2024) Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union, Luxembourg. DOI: https://doi.org/10.2813/442713

11. EuRepoc Data. European Repository of Cyber Incidents. Available at: https://eurepoc.eu/databases

12. Dzomira S. (2014) Digital forensic technologies as e-fraud risk mitigation tools in the banking industry: Evidence from Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions,* no. 4(2-1), pp. 116–124. DOI: https://doi.org/10.22495/rgcv4i2c1art4

13. Prasanthi B. V., Kanakam P., Hussain S. M. (2017) Cyber Forensic Science to Diagnose Digital Crimes-A study. *International Journal of Computer Trends and Technology*, no. 50(2), pp. 107–113. DOI: https://doi.org/10.14445/22312803/ijctt-v50p119

14. Singh S., Kumar S. (2020) Qualitative Assessment of Digital Forensic Tools. *Asian Journal of Electrical Sciences*, no. 9(1), pp. 25–32. DOI: https://doi.org/10.51983/ajes-2020.9.1.2372

15. Singh S., Singh V. K. (2023) Digital Forensic Investigation: Ontology, Methodology, and Technological Advancement. In Advancements in Cybercrime Investigation and Digital Forensics. Apple Academic Press. Pp. 137–160. DOI: https://doi.org/10.1201/9781003369479-7

16. Benjamine B. C., Subramaniam S. (2019) Enhancing the Financial Sector's Cyber Security in the Digital Economy. *Financial Stability Review,* pp. 44–46. Available at: https://www.bnm.gov.my/documents/20124/6433062/fsr2019h1_en_box2.pdf

Стаття надійшла до редакції 13.09.2024