УДК 004.056:343.9:355.4
JEL classification: D74; H56; L86; K42; O33
https://doi.org/10.31891/dsim-2024-7(32)

МЕХАНІЗМИ РОЗВИТКУ КІБЕРЗЛОЧИННОЇ ДІЯЛЬНОСТІ У ВОЄННИЙ ПЕРІОД

ПЕЛИХ Матвій
Сумський державний університет
https://orcid.org/0009-0000-5515-7089
pelih.m.r@gmail.com
Науковий керівник: ТЮТЮНИК Інна
доктор економічних наук, доцент
Сумський державний університет

У статті узагальнено найбільш поширені механізми розвитку кіберзлочинної діяльності, визначено її специфіку у воєнний період та ключові загрози, що постають перед державними інституціями, критичною інфраструктурою та суспільством внаслідок використання цифрових технологій у військових цілях. Мета дослідження полягає у висвітленні специфіки кіберзлочинності в умовах воєнних конфліктів, а також у систематизації механізмів і інструментів, які використовуються для кібератак на критичну інфраструктуру та фінансові системи. У дослідженні за допомогою методів контент-аналізу та порівняльного аналізу виявлено тренди і механізми розвитку кіберзлочинної діяльності, на основі інструментів системного аналізу здійснено оцінювання взаємозв'язків між різними аспектами кіберзлочинності (атаки на критичну інфраструктуру, інформаційні операції, фінансові злочини) та їх впливу на загальну безпеку держави, за допомогою статистичного аналізу здійснено узагальнення кількісних даних щодо кібератак та порівняння динаміки розвитку кіберзлочинності в мирний та воєнний часи. Результати аналізу свідчать про значне збільшення кількості кібератак на критичну інфраструктуру, урядові та військові об'єкти, а також поширення дезінформаційних кампаній. У дослідженні виявлено, що кіберзлочинні угруповання часто використовуються як інструмент державної стратегії в гібридній війні. Використання криптовалют у фінансових злочинах є однією з головних тенденцій, що ускладнює боротьбу з кіберзлочинністю через відсутність ефективних регуляторних механізмів. Результати дослідження можуть бути використані для розробки нових стратегій кібербезпеки в умовах війни, а також для покращення регулятивних і правових механізмів у сфері захисту від кібератак та фінансових злочинів, пов'язаних із криптовалютами.

Ключові слова: кіберзлочинність; гібридна війна; кібератаки; критична інфраструктура; криптовалюти; фінансові злочини; кібербезпека; дезінформація.

MECHANISMS OF CYBERCRIMINAL ACTIVITY DEVELOPMENT DURING WARTIME

PELIH Matvii
Sumy State University

The article summarizes the most common mechanisms of the development of cybercriminal activity, defines its specificity in the wartime period and the key threats facing state institutions, critical infrastructure and society as a result of the use of digital technologies for military purposes. The purpose of the study is to highlight the specifics of cybercrime in the context of military conflicts, as well as to systematize the mechanisms and tools used for cyberattacks on critical infrastructure and financial systems. In the study, using the methods of content analysis and comparative analysis, the trends and mechanisms of the development of cybercriminal activity were revealed, based on the tools of system analysis, an assessment of the interrelationships between various aspects of cybercrime (attacks on critical infrastructure, information operations, financial crimes) and their impact on the general security of the state, with the help of statistical analysis, quantitative data on cyberattacks and a comparison of the dynamics of the development of cybercrime in peacetime and wartime were carried out. The results of the analysis indicate a significant increase in the number of cyber attacks on critical infrastructure, government and military facilities, as well as the spread of disinformation campaigns. The study found that cybercriminal groups are often used as a tool of state strategy in hybrid warfare. The use of cryptocurrencies in financial crimes is one of the main trends, which complicates the fight against cybercrime due to the lack of effective regulatory mechanisms. The results of the research can be used to develop new cyber security strategies in the conditions of war, as well as to improve regulatory and legal mechanisms in the field of protection against cyber attacks and financial crimes related to cryptocurrencies.

Keywords: cybercrime; hybrid warfare; cyberattacks; critical infrastructure; cryptocurrencies; financial crimes; cybersecurity; disinformation.

ПЕЛИХ, М. (2024). МЕХАНІЗМИ РОЗВИТКУ КІБЕРЗЛОЧИННОЇ ДІЯЛЬНОСТІ У ВОЄННИЙ ПЕРІОД. *Development Service Industry Management*, (3), 219–222. https://doi.org/10.31891/dsim-2024-7(32)

PELIH, M. (2024). MECHANISMS OF CYBERCRIMINAL ACTIVITY DEVELOPMENT DURING WARTIME. *Development Service Industry Management*, (3), 219–222. https://doi.org/10.31891/dsim-2024-7(32)

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах розвитку суспільно-економічних та політичних відносин з кожним роком дедалі більшого значення у вирішенні конфліктів, у тому числі і військових, набуває цифровий простір. Переважна більшість сучасних військово-політичних конфліктів супроводжується не лише зміною традиційних форм їх

ведення та вирішення, але й активним розширенням переліку механізмів їх реалізації. Цифрові технології стають одним із найбільш впливових інструментів здійснення атак на стратегічні об'єкти розвитку та функціонування країни: об'єкти критичної інфраструктури, інформаційні та платіжні системи тощо, а кіберзлочинність – багатофункціональним інструментом, що здійснює суттєвий вплив на національну безпеку, хід проведення військових операцій, стабільність та безпеку інформаційного середовища країни.

Ще більшої актуальності дослідження механізмів розвитку кіберзлочинності у воєнний період набувають в умовах зростаючої залежності суспільства від цифрових технологій та інформаційної інфраструктури. Виходячи за межі традиційних полів бою, військові дії все частіше переносяться в кіберпростір, що робить кіберзлочинність не лише важливим інструментом боротьби між державами, але й засобом впливу на їх економічну та політичну стабільність. Під час воєнних дій кібератаки посилюють дестабілізацію критичних секторів економіки, порушують стабільність функціонування державних інституцій та підривають довіру громадян до системи публічного управління. Таким чином, дослідження механізмів здійснення кіберзлочинної діяльності в умовах війни є надзвичайно важливим елементом їх ідентифікації та розробки ефективних заходів протидії ним.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналіз існуючих теоретичних та прикладних досліджень, присвячених питанням кіберзлочинності у воєнний період, засвідчує зростаючу роль даних питань у забезпеченні безпеки країни. Т. Рід [**Помилка! Джерело посилання не знайдено.**] та Л. Келло [**Помилка! Джерело посилання не знайдено.**] розглядають кіберзлочинність як основну арену військових дій, на якій державні та недержавні гравці здійснюють кібератаки для досягнення стратегічних цілей без прямого військового втручання. У роботах Д. Кавелті [**Помилка! Джерело посилання не знайдено.**] та F-Secure [**Помилка! Джерело посилання не знайдено.**] проведено аналіз кібератак на критичну інфраструктуру під час військових конфліктів та доведено їх катастрофічні наслідки для економіки та соціальної стабільності країн, що воюють. Використання децентралізованих цифрових валют для фінансування незаконних дій, особливо в періоди нестабільності та конфліктів досліджено у роботі С. Фолі, Дж. Р. Карлсена, Т. Дж. Путнінса [**Помилка! Джерело посилання не знайдено.**].

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Незважаючи на значний інтерес науковців до даної проблематики, багато аспектів розвитку кіберзлочинної діяльності у воєнний період залишаються недостатньо вивченими. Зокрема, подальшого дослідження потребують питання появи нових схем злочинної діяльності у кіберпросторі, а також розробки ефективних правових механізмів регулювання та захисту кіберпростору в умовах конфліктів.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою даного дослідження є узагальнення найбільш поширених механізмів розвитку кіберзлочинної діяльності, визначення специфіки такої діяльності у воєнний період та виявлення ключових загроз, що постають перед державними інституціями, критичною інфраструктурою та суспільством внаслідок використання цифрових технологій.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У періоди нестабільності та військових протистоянь кіберзлочинна діяльність набуває специфічних форм прояву і часто стає одним із ключових елементів ведення війни. Характер операцій в кіберпросторі надає зловмисникам можливість забезпечити анонімність та мінімізувати витрати їх проведення, прискорити швидкість їх здійснення та значно ускладнити процедури їх моніторингу та контролю. Це робить злочинність в кіберпросторі ефективним інструментом порушення економічної, соціальної та політичної стабільності країни.

Одним із найбільш поширених та актуальних інструментів здійснення кіберзлочинної діяльності з урахуванням специфіки війни в Україні є атаки на критичну інфраструктуру. З метою впливу на хід ведення війни і настрої суспільства кіберзлочинці можуть здійснювати атаки на енергетичні, транспортні, фінансові та телекомунікаційні системи та інші критично важливі об'єкти інфраструктури, що в кінцевому результаті може мати катастрофічні наслідки для стабільного функціонування держави. Так, за даними Державної служби спеціального зв'язку та захисту інформації України [**Помилка! Джерело посилання не знайдено.**], з початку російського вторгнення в Україну кількість кібератак на критичну інфраструктуру зросла на 400% порівняно з довоєнними роками. Лише у 2022 році, пов'язаними з російськими хакерськими угрупованнями кіберзлочинцями, було здійснено низку атак на українську енергетичну інфраструктуру, серед яких значну частку займали атаки на операторів енергомереж.

Не менш важливою і поширеною складовою кіберзлочинної діяльності в умовах війни є інформаційні кампанії, що спрямовані на поширення неправдивої інформації, маніпуляції у соціальних мережах, створення фейкових новин і підриву довіри до офіційних джерел інформації. Дана діяльність стає невід'ємною частиною

сучасних психологічних операцій, що спрямовані на дестабілізацію суспільства. За даними Державної служби спеціального зв'язку та захисту інформації України [**Помилка! Джерело посилання не знайдено.**], лише у 2022 році кількість кіберінцидентів в Україні зросла у 2,8 разів, а кількість кампаній з дезінформації перевищувала 200.

В умовах активного розвитку цифрових валют суттєву роль у фінансуванні незаконних операцій починають займати криптовалюти. Згідно з дослідженням FATF, у 2022 році частка криптовалютних транзакцій, що пов'язані з незаконною діяльністю зросла до 2,1%. Стрімке зростання ролі криптовалют у злочинній діяльності в цифровому просторі зумовлено складністю відстеження транзакцій і постійними змінами схем їх здійснення. Це значно ускладнює роботу правоохоронних органів у боротьбі з фінансовими злочинами та актуалізує питання розробки нових інструментів та підходів до регулювання цих процесів.

Результати проведеного European Banking Authority дослідження [**Помилка! Джерело посилання не знайдено.**] засвідчують, що однією із головних проблем контролю за використанням криптовалюти слугує відсутність гармонізованої правової бази. Швидкий розвиток технологій блокчейну призводить до того, що регулятори не встигають адаптувати свої законодавчі ініціативи до реалій функціонування фінансової системи, тим самим створюючи сприятливі можливості до використання злочинцями криптовалюти для нелегальних фінансових операцій.

Значний вплив на ефективність своєчасної ідентифікації злочинних операцій в кіберпросторі здійснюють інноваційні технології. Активне використання кіберзлочинцями технологій штучного інтелекту, машинного навчання та автоматизованих атак дозволяє їм підвищувати ефективність своїх дій та уникати покарання.

Дослідження С. Амбасадорса [**Помилка! Джерело посилання не знайдено.**] акцентує увагу на ролі штучного інтелекту в процесі виявлення підозрілих транзакцій у криптовалютних мережах. Аналіз особливостей використання машинного навчання для аналізу великих масивів даних у біткоїн-мережах продемонстрував позитивний вплив на швидкість та якість виявлення фінансових операцій з відмивання грошей. За результатами дослідження доведено ефективність застосування інноваційних технологій, серед яких штучний інтелект та аналіз великих даних, у протидії кіберзлочинності. Фахівці міжнародної організації FATF [**Помилка! Джерело посилання не знайдено.**] також підкреслюють важливість впровадження штучного інтелекту для посилення боротьби з фінансовими злочинами, включаючи нелегальні операції з криптовалютами.

У роботі П. Опітека, А. Бутор-Келера та К. Канклерза [**Помилка! Джерело посилання не знайдено.**] проведено детальний аналіз різних форм злочинної діяльності, що пов'язана з криптовалютами, серед яких відмивання грошей, шахрайство та фінансування тероризму. Авторами узагальнено проблеми в діяльності правоохоронних органів, що пов'язані із децентралізованим та анонімним характером криптовалют та ускладнюють процеси моніторингу та регулювання транзакцій. За результатами аналізу законодавчої бази та регулятивних заходів зроблено висновок про необхідність удосконалення підходів до боротьби з неправомірним використанням криптовалют.

К. Леупрехтом, К. Дженкінсом та Р. Гамілтоном [**Помилка! Джерело посилання не знайдено.**] досліджено роль криптовалют у схемах відмивання грошей та пов'язані з цим політичні виклики. Авторами зазначено, що децентралізована структура криптовалют робить їх привабливими для зловмисників в їх прагненні приховати походження незаконних коштів. Автори також наголошують на необхідності застосування більш жорсткої нормативно-правової бази та налагодження міжнародного співробітництва для ефективної боротьби зі зловживаннями у цій сфері.

Таким чином, аналіз ролі технологій штучного інтелекту, машинного навчання та аналізу великих даних у розвитку кіберзлочинності засвідчує необхідність подальшої розробки інноваційних технологій для ефективного виявлення злочинної діяльності в криптовалютних мережах, адаптації та приведення у відповідність діяльності регуляторних органів до темпів розвитку технологій, що дозволить знизити ризики економічної та політичної безпеки країни в умовах воєнних конфліктів.

У воєнний період найбільш поширеними об'єктами кібератак слугують Державні установи, військові об'єкти та органи правопорядку. Як правило метою даних атак слугує збір розвідувальної інформації, порушення комунікації та порядку. Викрадення конфіденційних даних урядових структур або військових планів дозволяє супротивнику отримати критично важливу інформацію для передбачення військових дій та підриву обороноздатності країни.

Крім того, значна частина таких атак спрямована на порушення ланцюгів управління, що веде до дезорганізації та втрати координації між державними інституціями та військовими підрозділами. За даними Державної служби спеціального зв'язку та захисту інформації України [**Помилка! Джерело посилання не знайдено.**], в перші місяці війни в Україні було зафіксовано понад 2 000 спроб кібератак на урядові сайти та системи управління військовими об'єктами, а кількість спрямованих на викрадення даних державних установ і підприємств оборонної промисловості атак зросла на 250%. Основними об'єктами таких атак були електронні системи управління військовими операціями, бази даних оборонних підприємств, а також пов'язані з дослідженнями та розробками у військовій сфері інформаційні ресурси.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Наведені дані дозволяють зробити висновок про те, що кіберзлочинність у воєнний період слугує стратегічним інструментом послаблення військового потенціалу супротивника та підвищення власних можливостей шляхом отримання доступу до критичної інформації. Вона є одним із ключових елементів гібридної війни. Завдяки низьким витратам, анонімності та децентралізованій природі цифрового простору, зловмисники можуть здійснювати кібератаки, які мають серйозні наслідки для економічної, соціальної та політичної стабільності держав. Кіберзлочинці активно використовують сучасні технології для атак на критичну інфраструктуру, інформаційні ресурси та фінансові системи.

Іншою серйозною проблемою є інформаційні атаки та поширення дезінформації, які підривають довіру до офіційних джерел інформації і сприяють деморалізації суспільства.

Фінансова кіберзлочинність, особливо із використанням криптовалют, також є важливою складовою кіберзлочинної діяльності у воєнний період. Використання криптовалют для відмивання грошей і фінансування незаконних операцій ускладнює роботу правоохоронних органів через відсутність чітких механізмів регулювання цієї сфери. Це підкреслює стратегічну важливість захисту військових і державних структур від кібератак, особливо в умовах сучасних воєнних конфліктів.

Загалом, ефективна протидія кіберзлочинності в умовах війни потребує активного використання новітніх технологій, таких як штучний інтелект і аналіз великих даних, а також тісної міжнародної співпраці для впровадження нових регулятивних підходів і механізмів боротьби з кіберзлочинами.

Робота виконана за підтримки Міністерства освіти і науки України за результатами проекту «Моделювання механізмів протидії організованій та транснаціональній кіберзлочинності у воєнний та післявоєнний часи» (реєстраційний номер 0124U000550).

References

1. Ambassadors S. (2024). Blockchain Transaction Detection with AI. Medium. URL: https://medium.com/@singularitynetambassadors/blockchain-transaction-detection-with-ai-32508414492f (дата звернення: 14.03.2024).
2. Dunn Cavelty M. (2014). Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, vol. 20(3), pp 701-15
3. EBA warns consumers on virtual currencies European Banking Authority. URL: https://www.eba.europa.eu/publications-and-media/press-releases/eba-warns-consumers-virtual-currencies (дата звернення: 14.03.2024).
4. Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France. URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-newtechnologies-aml-cft.html (дата звернення: 14.03.2024).
5. Foley S., Karlsen J. R., Putnins T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Review of Financial Studies*, vol. 32(5), pp. 1798-1853.
6. *Cyber threat landscape report 2021*. F-Secure Labs. URL: https://www.withsecure.com/content/dam/with-secure/en/investor/materials/annual-reports/2021/annual-report-2021.pdf (дата звернення: 14.03.2024).
7. Juels A., Kosba A., Shi E. (2016). The ring of gyges. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*.
8. Kello L. (2017). *The Virtual Weapon and International Order*. Yale University Press.
9. Kethineni S., Cao Y. (2019). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, vol. 30(3), pp. 325–344.
10. Leuprecht C., Jenkins C., Hamilton R. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, vol. 30(4), pp. 1036-1054.
11. McGinn D., Birch D., Akroyd D., Molina-Solana M., Guo Y., Knottenbelt W. J. (2016). Visualizing Dynamic Bitcoin Transaction Patterns. *Big Data*, vol. 4(2), pp. 109–119.
12. Opitek P., Butor-Keler A., Kanclerz K. (2023). Selected aspects of crime involving virtual currencies. *Terroryzm*, vol. 4(4), pp. 325–376.
13. Rid T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, vol. 35(1), pp. 5–32.
14. Wu L., Hu Y., Zhou Y., Wang H., Luo X., Wang Z., Zhang F., Ren K. (2021). Towards understanding and demystifying Bitcoin Mixing Services. *Proceedings of the Web Conference*.
15. State Service of Special Communications and Information Protection of Ukraine. URL: https://cip.gov.ua/ua (access date Marth 14, 2024).