УДК 343.1:004
DOI https://doi.org/10.32689/2522-4603.2023.3.7

Володимир ПОЛІЩУК
аспірант Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, Київ, Україна, 03039, Polishchuk.Volodymyr.20@proton.me
ORCID: 0009-0002-2642-9326

Volodymyr POLISHCHUK
Postgraduate Student at the Interregional Academy of Personnel Management, 2, Frometivska St, Kyiv, Ukraine, 03039, Polishchuk.Volodymyr.20@proton.me
ORCID: 0009-0002-2642-9326

КІБЕРЗЛОЧИНИ ТА КІБЕРБЕЗПЕКА: БОРОТЬБА З КОМП'ЮТЕРНИМИ ЗЛОЧИНАМИ І КІБЕРАТАКАМИ

CYBERCRIMES AND CYBER SECURITY: COMBATING COMPUTER CRIMES AND CYBERATTACKS

Анотація. *Дана робота досліджує різні типи кіберзлочинів та їхні особливості, а також методи та інструменти, які використовуються кіберзлочинцями, а також заходи, які можна вжити для захисту від кіберзлочинів; роль правоохоронних органів та міжнародної співпраці у боротьбі з кіберзлочинністю. Автор розглядає актуальні тенденції та прогнози розвитку кіберзлочинності в Україні та міжнародний досвід боротьби із кіберзлочинами.*

У роботі зроблена спроба ознайомитися з розвитком нових форм вчинення кіберзлочинів у контексті історичного розвитку.

Кіберзлочини часто складні для розслідування через брак кваліфікованих кадрів, необхідних інструментів та міжнародної співпраці. Кіберзлочинці часто ховаються за анонімністю, що ускладнює їх ідентифікацію та притягнення до відповідальності. Законодавство у сфері кіберзлочинності постійно еволюціонує, адже не завжди встигає за темпами розвитку нових технологій. Важливо зазначити, що кіберзлочинність є серйозною загрозою для суспільства, тому необхідні спільні зусилля держави, приватного сектору та громадян для її подолання.

Боротьба з кіберзлочинністю та забезпечення кібербезпеки – одна із найактуальніших проблем сьогодення. Це питання, яке потребує комплексного підходу, що містить як правові, так і технічні аспекти.

Очікуваними результатами роботи є:

– Визначення та систематизація основних понять кіберзлочинності та кібербезпеки.

– Розробка типології кіберзлочинів.

– Узагальнення та аналіз методів та інструментів кіберзахисту.

– Визначення шляхів удосконалення діяльності правоохоронних органів у сфері боротьби з кіберзлочинністю.

– Обґрунтування рекомендацій щодо розвитку кібербезпеки.

– Результати дослідження можуть бути використані для розробки та вдосконалення політики кібербезпеки на державному та приватному рівні.

Розслідування кібератак як воєнних злочинів може допомогти притягнути винних до відповідальності, а також запобігти подібним злочинам у майбутньому.

Ключові слова: *кіберзлочинність, кібербезпека, комп'ютерні злочини, кібератаки, шахрайство, крадіжка особистих даних, шпигунство, критична інфраструктура, захист інформації, правоохоронні органи, міжнародна співпраця.*

Abstract. *This paper examines the different types of cybercrimes and their characteristics, as well as the methods and tools used by cybercriminals, as well as measures that can be taken to protect against cybercrimes; the role of law enforcement agencies and international cooperation in the fight against cybercrime. The author examines current trends and forecasts of the development of cybercrime in Ukraine and international experience in combating cybercrime.*

The work attempts to familiarize with the development of new forms of committing cybercrimes in the context of historical development.

Cybercrimes are often difficult to investigate due to a lack of skilled personnel, necessary tools and international cooperation. Cybercriminals often hide behind anonymity, making it difficult to identify and prosecute them. Legislation in the field of cybercrime is constantly evolving, because it does not always keep up with the pace of development of new technologies. It is important to note that cybercrime is a serious threat to society, therefore joint efforts of the state, private sector and citizens are necessary to overcome it.

Fighting cybercrime and ensuring cyber security is one of the most urgent problems today. This is an issue that requires a comprehensive approach that includes both legal and technical aspects.

The expected results of the work are:
– Definition and systematization of the main concepts of cybercrime and cyber security.
– Development of a typology of cybercrimes.
– Generalization and analysis of cyber protection methods and tools.
– Determination of ways to improve the activities of law enforcement agencies in the field of combating cybercrime.
– Justification of recommendations for the development of cyber security.
– Research results can be used to develop and improve cyber security policy at the state and private level.
Investigating cyber-attacks as war crimes can help bring perpetrators to justice and prevent similar crimes in the future.
Key words: *cyber-crime, cyber security, computer crimes, cyber-attacks, fraud, identity theft, espionage, critical infrastructure, information protection, law enforcement, international cooperation.*

Постановка проблеми. У сучасному світі, де все більше аспектів життя переходить в онлайн, кіберзлочинність та кібербезпека стають актуальними питаннями.

Згідно з даними ФБР, у 2022 році зареєстровано 800 944 скарги на кіберзлочинність. Це означає, щонайменше 422 мільйони людей постраждали від цього негативного явища. У 2023 році зламано майже 33 мільярди облікових записів [1], вартість яких оцінено у 8 трильйонів доларів. Кіберзлочинність – індустрія злочинців, яка коштує трильйони доларів, і 43% атак спрямовані на малий і середній бізнес. Протягом останніх двадцяти років, у період з 2001 по 2021 роки кіберзлочинність забрала щонайменше 6,5 мільйонів жертв. За цей самий період сума збитків склала майже 26 мільярдів доларів.

На думку експертів видання Cybercrime Magazine у наступні п’ять років витрати від кіберзлочинності зростуть на 15% і до 2025 року досягнуть 10,5 трлн. Програми-вимагачі щороку коштують своїм жертвам близько 265 мільярдів доларів США [4]. 80% зареєстрованих кіберзлочинів зазвичай пов’язані з фішинговими атаками в технологічному секторі. Це значна проблема, яка потребує негайного вирішення спільними зусиллями, оскільки кіберзлочини, такі як шахрайство, крадіжка особистих даних, шпигунство та атаки на критичну інфраструктуру, можуть мати значні наслідки як для окремих осіб, так і для цілих організацій та держав.

Мета роботи – дослідження проблем кіберзлочинності та кібербезпеки, а також аналіз шляхів боротьби з комп'ютерними злочинами й кібератаками.

Для досягнення мети роботи передбачається вирішити наступні завдання:

– проаналізувати типи та особливості кіберзлочинів;

– розглянути методи та інструменти кіберзахисту;

– визначити актуальні проблеми та перспективи розвитку кібербезпеки.

Кіберзлочинність постійно змінюється, постійно виникають нові типи злочинів та використовуються нові технології. Загалом цей процес можна поділити на кілька етапів розвитку. На початку шістдесятих з'являються перші комп'ютерні мережі, що дає поштовх до розвитку кіберзлочинності. Саме тоді почалися і перші випадки крадіжки даних та комп'ютерних програм. У вісімдесятих набули поширення персональні комп'ютери та Інтернет. І у цей період з'являються перші кіберзлочинні групи, які використовують кібершантажу та викрадення даних. У 1990-ті відбулося стрімке зростання кіберзлочинності, перші масштабні кібератаки. З'являються нові типи кіберзлочинів [2]. На початку 2020 спостерігається різке зростання кількості кібератак на державні органи та приватні компанії. Кібербезпека стає одним з пріоритетів національної безпеки. Кіберзлочинність стає все більш витонченою та складною. Зростає кількості кібератак на штучний інтелект та інші нові технології.

Перше покоління кіберзлочинів включає атаки, спрямовані на комп’ютери, комп’ютерні мережі та дані.

Друге покоління пов'язане з розвитком IT-мереж і атаками хакерів на їх цілісність і доступність.

Третє покоління пов'язане з помітним процесом автоматизації кіберзлочинності, що є, в тому числі результатом використання спеціального програмного забезпечення[3].

Нове покоління кіберзлочинів не вчиняється особисто та безпосередньо злочинцями, а є результатом автоматизованих атак з використанням програмного забезпечення, створеного для цієї мети.

Разом з тим, намагаючись постійно розв'язувати проблеми кібератак, фахівці розробили сучасні методи кіберзахисту, до яких відносять:

1. Запобігання кібератакам шляхом впровадження відповідних заходів безпеки.

2. Своєчасне виявлення кібератак для мінімізації їхніх наслідків.

3. Заходи для нейтралізації кібератак та відновлення роботи систем.

Серед інструментів кіберзахисту найчастіше використовують антивірусне програмне забезпечення, яке захищає комп'ютерні системи від

вірусів, шпигунських програм та інших шкідливих програм [5]. Брандмауер – теж один з інструментів захисту, який блокує несанкціонований доступ до комп'ютерних систем.

Системи запобігання вторгненням блокують підозрілу активність у комп'ютерних мережах [5]. Метод шифрування захищає дані від несанкціонованого доступу через використання спеціальних шифрів та обмежує доступ до комп'ютерних систем та даних. Не варто забувати й про підвищення обізнаності користувачів щодо ризиків кіберзлочинності, які спрямовані на захист себе від них [5]. Враховуючи загрози сьогодення важливо використовувати комплексний підхід до кіберзахисту, який поєднує різні методи та інструменти. Зважаючи на ряд актуальних проблем кібербезпеки можемо виділити наступне:

Кіберзлочинці постійно вдосконалюють свої методи, що робить кібератаки все більш складними для виявлення та нейтралізації [6].

Існує гостра нестача фахівців з кібербезпеки, що ускладнює захист організацій від кібератак.

Різні організації та країни мають різні підходи до кібербезпеки, що ускладнює міжнародну співпрацю [7].

Зростання залежності від Інтернету робить суспільство більш вразливим до кібератак.

Кіберзлочинність постійно еволюціонує, з'являються нові типи кіберзлочинів, що потребує постійного вдосконалення методів боротьби з ними [8].

Штучний інтелект може допомогти у виявленні та нейтралізації кібератак. Зростання обізнаності про кібербезпеку допоможе людям краще захищати себе від кіберзлочинності. Рухаючись у напрямі міжнародної співпраці кожна країна може допомогти собі у боротьбі з транснаціональною кіберзлочинністю. Вдосконалення законодавства сприятиме забезпеченню ефективного розслідування та переслідування злочинців [9].

Висновки. Кібератаки стають все більш витонченими та складними, що робить кібербезпеку критично важливою. Ефективна боротьба з кіберзлочинністю потребує співпраці між державами, приватним сектором та громадянами. Необхідно постійно вдосконалювати методи кібербезпеки, використовуючи нові технології та підвищуючи обізнаність. Важливо розробити міжнародні стандарти та законодавство для боротьби з транснаціональною кіберзлочинністю. Майбутнє кібербезпеки залежить від здатності різних зацікавлених сторін працювати разом для захисту інформаційних систем та даних.

Література:

1. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал.* 2012. № 12. С. 409–414.

2. Музика В. В. Атрибуція кібератак проти об’єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення : дис. … д-ра філософії : 081 / Нац. ун-т. «Одеська юридична академія». Одеса, 2021. 219 с.

3. Фещуков Г. В. Застосування МГП по відношенню до кібероперацій, що проводяться під час збройних конфліктів. *Юридичний науковий електронний журнал*. 2023. № 9. С. 437–439.

4. Geers K. Strategic cyber security : Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2011. 169 p.

5. The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris : веб-сайт. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russiascyberwar-against-ukraine/ (дата звернення: 25.02.2024).

6. The Prosecutor’s New Policy on ‘Cyber Operations’ before the International Criminal Court (and its Implications for Ukraine). Blog of the European Journal of International Law: веб-сайт. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-theinternational-criminal-court-and-its-implications-for-ukraine-some-preliminaryreflections/ (дата звернення: 25.02.2024).

7. Information for victims. International Criminal Court : веб-сайт. URL: https://www.icc-cpi.int/victims/ukraine (дата звернення: 25.02.2024).

8. Римський статут Міжнародного кримінального суду. *Міністерство юстиції України* : веб-сайт. URL: https://minjust.gov.ua/m/ mijnarodniy-kriminalniy-sud (дата звернення: 25.02.2024).

9. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare / Michael N. – Cambridge University Press (дата звернення: 25.02.2024).

References:

1. Yurtayeva, K. V. (2012). Kryminal′na vidpovidal′nist′ za kiberzlochyny, vchyneni pid chas zbroynoho konfliktu: mizhnarodni tendentsiyi ta ukrayins′ki realiyi [Criminal liability for cybercrimes committed during armed conflict: international trends and Ukrainian realities]. *Yurydychnyy naukovyy elektronnyy zhurnal – Legal scientific electronic journal,* 12, 409–414.

2. Music, V. V. (202). Atrybutsiya kiberatak proty ob″yektiv krytychnoyi infrastruktury: vyznachennya osnovnykh problem ta shlyakhiv yikh vyrishennya : dys. … d-ra filosofiyi : 081 [Attribution of cyber attacks against critical infrastructure objects: definition of the main problems and ways to solve them: diss. ... doctor of philosophy: 081]. *Nats. un-t. «Odes'ka yurydychna akademiya». Odesa – Nat. Univ. "Odesa Law Academy". Odesa*, 219.

3. Feshchukov, G. V. (2023). Zastosuvannya MHP po vidnoshennyu do kiberoperatsiy, shcho provodyat′sya pid chas zbroynykh konfliktiv [Application of IHL in relation to cyber operations conducted during armed conflicts]. *Yurydychnyy naukovyy elektronnyy zhurnal – Legal scientific electronic journal*, 9, 437–439.

4. Geers, K. (2011). Strategic cyber security: Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 169.

5. The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris : Website. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russiascyberwar-against-ukraine/ (access date: 02/25/2024).

6. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine). Blog of the European Journal of International Law: website. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-theinternational-criminal-court-and-its-implications-for-ukraine-some-preliminaryreflections/ (date application: 25.02.2024).

7. Information for victims. International Criminal Court : website. URL: https://www.icc-cpi.int/victims/ukraine (access date: 25.02.2024).

8. Ryms′kyy statut Mizhnarodnoho kryminal′noho sudu [Rome Statute of the International Criminal Court]. *Ministerstvo yustytsiyi Ukrayiny: veb-sayt – Ministry of Justice of Ukraine: website.* URL: https://minjust.gov.ua/m/ mijnarodniy-kriminalniy-sud (date of application: 02/25/2024).

9. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare / Michael N. Cambridge University Press (access date: 25.02.2024).