ВИКЛИКИ КІБЕРБЕЗПЕКИ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ У ЦИФРОВУ ЕПОХУ

БУРБИКА Віталій Олександрович - кандидат юридичних наук,
https://orcid.org/0009-0007-5615-8121
УДК 347.97
DOI: https://doi.org/10.32782/ep.2024.1.38

У сучасному світі, де цифрові технології стрімко розвиваються та проникають у всі сфери життя, правоохоронні органи стикаються з новими викликами у сфері кібербезпеки. Визначено, що злочинці все частіше використовують кіберпростір для вчинення протиправних дій, що ставить під загрозу безпеку держави, бізнесу та громадян. Тому правоохоронним органам необхідно адаптуватися до цих змін та розробляти ефективні стратегії протидії кіберзлочинності.

Проблема кібербезпеки та виклики, пов'язані з кіберзлочинністю для правоохоронних органів, є предметом активного дослідження в сучасній науковій літературі. Багато досліджень присвячені аналізу загроз кібербезпеці та розробці стратегій їх подолання. Проте, є потреба в подальших дослідженнях для розробки нових підходів та стратегій боротьби з кіберзлочинністю в умовах швидкого технологічного розвитку.

Проведено дослідження актуальних проблем, які виникають перед правоохоронними органами у зв'язку зі зростанням кіберзагроз у сучасному цифровому світі. Аналізується широкий спектр викликів, що постають перед правоохоронцями в сфері кібербезпеки, таких як кібератаки, кібершпигунство, кібертероризм тощо. У статті також розглядаються стратегії та методи боротьби з кіберзагрозами, включаючи вдосконалення технічних засобів захисту, підвищення кваліфікації персоналу та розвиток міжнародного співробітництва у сфері кібербезпеки. Завдяки системному аналізу та висвітленню сучасних тенденцій у цій галузі, даний напрям досліджень сприяє кращому розумінню складнощів і перспектив розвитку кібербезпеки в контексті діяльності правоохоронних органів.

В результаті роботи визначено, що важливо провести докладне вивчення сучасного стану кібербезпеки України в умовах військового конфлікту та розуміти необхідність захисту кіберпростору в умовах загрози війни. Здатність країни ефективно захищати свої інформаційні активи під час військових конфліктів стає вирішальним фактором для забезпечення національної безпеки та стимулювання економічного розвитку.

Ключові слова: кібербезпека, кіберзлочинність, правоохоронні органи, воєнний стан, національна безпека.

Метою статті є комплексний аналіз основних викликів у сфері кібербезпеки для правоохоронних органів в епоху цифрових технологій та визначення ефективних шляхів для їх подолання.

Стан наукової дослідженості

На сьогодні є численні наукові публікації, присвячені загальним питанням кібербезпеки, кіберзлочинності та діяльності правоохоронних органів у цій сфері. Питанням забезпечення кібербезпеки приділяли значну увагу науковці-правники, такі як О. Панченко, І. Бінько, В. Шевчук, Б. Кормич, Ю. Уфімцев, В. Буянов, Е. Єрофеєв. Проте, ця тема досі залишається недостатньо вивченою, а дослідження функціонування правоохоронних органів у галузі забезпечення кібербезпеки продовжує бути актуальним.

Виклад основного матеріалу

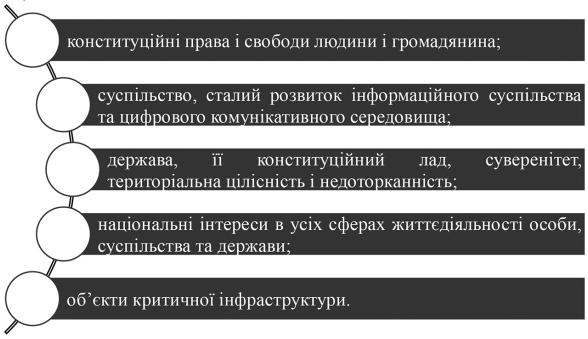
У сучасному світі кібербезпека стала однією з ключових складових національної безпеки, особливо в умовах воєнного стану. В Україні, зокрема, питання захисту кіберпростору набуло надзвичайної важливості через триваючу агресію та пов'язані з нею кібератаки на критичну інфраструктуру, державні установи та приватний сектор. Військові конфлікти значно ускладнюють ситуацію, створюючи нові виклики для захисту інформаційних ресурсів і вимагаючи від держави та її правоохоронних органів постійної готовності до відбиття кіберзагроз.

Правоохоронні органи відіграють ключову роль у боротьбі з кіберзлочинністю, забезпечуючи дотримання законів у кіберпросторі та захищаючи громадян і організації від кіберзагроз. Однак вони стикаються з численними викликами, які ускладнюють їхню діяльність у цій сфері.

Сам термін «кібербезпека» тлумачиться законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, та означає захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Зокрема, у статті 4 п. 1 згаданого закону виділяються об'єкти кібербезпеки, які включають:

Схема 1. Об'єкти кібербезпеки та кіберзахисту.



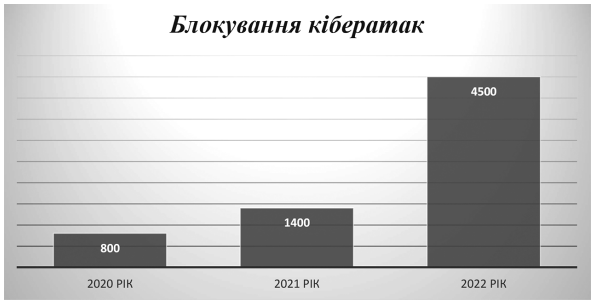
Створено автором на основі [1].

Відповідно суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності та ін.

За словами начальника Департаменту кібербезпеки СБУ, Іллі Вітюка, «Після початку повномасштабного вторгнення російські хакери здійснюють по 4,5 тис. кібератак щороку». Також виокремлює, що кібервійна набирає обертів. «Адже у 2015-2016 роках у нас були перші деструктивні атаки по об'єктах енергетики. Потім був вірус NotPetya, тривали постійні DDoS-атаки, були спроби проникнень. СБУ все це відбивала і постійно аналізувала», – сказав він [2].

Вітюк зазначив, що Росія довгий час розвивала свій кібернаступальний потенціал і почала активно використовувати його після початку повномасштабного вторгнення. «Наприклад, у 2020 році ми заблокували 800 кібератак, у 2021 році – 1400, а після початку повномасштабної війни їх кількість зросла до 4500 щороку», – уточнив він. За словами Вітюка, фахівці СБУ зупинили багато небезпечних спроб проникнути в системи зв'язку Збройних сил та Міністерства оборони України [2].

Діаграма 1. Протидія російським кібератакам.



Створено автором на основі [2].

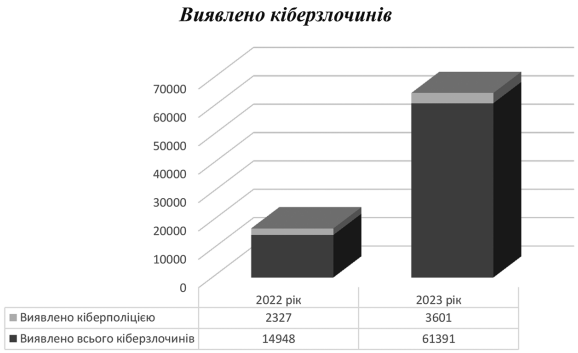
Зокрема і підрозділи кіберполіції долучені до забезпечення кібероборони України та виконання завдань з кіберборотьби проти збройної агресії російських військ. Зокрема, кіберполіцією у 2023 році забезпечено блокування близько 2,9 тис. важливих інформаційних ресурсів рф та рб (урядових

сайтів, банківської та медіасфери, авіаперевезень тощо) [3, с. 5].

Статистика вказує на значне зростання кількості виявлених кримінальних правопорушень у сфері високих інформаційних технологій порівняно з попереднім періодом. Кількість таких злочинів зросла в 4,1 рази – з 14,9 тисяч до 61,4 тисяч випадків. Особливо стрімко зросла кількість онлайн-шахрайств, збільшившись у 5,8 разів – з 7,9 тисяч до 45,7 тисяч випадків. Водночас, правоохоронним органам вдалося розкрити на 91% більше кіберзлочинів – з 7,3 тисяч до 13,9 тисяч випадків. У банківській сфері кількість розкритих злочинів зросла на 12% (з 2,1 тисячі до 2,4 тисячі), у сфері комп'ютерних систем – на 44% (з 1,3 тисячі до 1,9 тисячі). Значно збільшилася кількість розкритих правопорушень у сфері телекомунікацій та протиправного контенту – у 3,2 рази (зі 101 до 323 випадків), а також онлайн-шахрайств – у 3,9 рази (з 1,7 тисячі до 6,7 тисячі випадків) [3, с. 9].

Також забезпечено ефективне відшкодування збитків, завданих кіберзлочинами. У 2023 році відшкодовано 286,8 млн грн, що у 6,4 рази більше ніж у 2022 р. – 44,5 млн грн

Діаграма 2. Розкриття кіберполіцією кіберзлочинів



Створено автором на основі [3].

Українські правоохоронні органи опинилися на передовій цієї кібервійни, відбиваючи численні атаки та намагаючись забезпечити кібербезпеку в умовах воєнного стану. Ця ситуація створює додаткові виклики для них, але крім атаки рф це не єдині складнощі.

Спеціалісти ESET (експерт у сфері захисту від кіберзлочинності та цифрових загроз, розробник рішень у сфері IT-безпеки та провідний постачальник технологій для виявлення загроз. Заснована у 1992 році, ESET сьогодні має широку партнерську мережу та представництва у більш ніж 180 країнах світу. Головний офіс компанії розташований у Братиславі, Словаччина) виділяють основні виклики, які постають перед кібербезпекою вже зараз та виникнуть у найближчому майбутньому:

Висновок

Сучасні виклики кібербезпеки вимагають від правоохоронних органів постійного вдосконалення та адаптації до нових умов. Високий рівень технічної підготовки, впровадження новітніх технологій та тісна співпраця на всіх рівнях є ключовими факторами успішної протидії кіберзлочинності. Забезпечення кібербезпеки в цифрову епоху – це не тільки захист інформаційних систем, а й гарантія національної безпеки та стабільності держави.

Водночас Україна робить усе можливе для зміцнення своєї кібербезпеки. Приймаються нові закони та стратегії, створюються спеціалізовані підрозділи, розвивається співпраця з провідними кібербезпековими організаціями. Крім того, посилюється підготовка кадрів та підвищується обізнаність населення щодо кіберзагроз. Незважаючи на всі виклики, українські правоохоронні органи демонструють стійкість та рішучість у боротьбі з кіберзлочинністю. Досвід, отриманий під час воєнного конфлікту, дозволить краще підготуватися до майбутніх кіберзагроз і забезпечити безпеку цифрового середовища в Україні на належному рівні.

Література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Від початку війни російські хакери здійснюють по 4,5 тисячі кібератак щороку - СБУ. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-technology/3848393-vid-

Таблиця 1. Основні виклики, які постають перед кібербезпекою вже зараз та виникнуть у найближчому майбутньому.

№ з/п	Виклик	Роз'яснення
1.	Збільшення кількості кібератак	Згідно зі звітом Cybersecurity Ventures, глобальні збитки від кіберзлочинної діяльності очікується, що зростатимуть на 15% щороку з 2021 до 2025 року і можуть досягти 10,5 трильйонів доларів на рік. Це зростання обумовлене значною активністю кіберзлочинних груп і зловмисників, діяльність яких спонсорується державою. Одночасно, кількість атак збільшується через процеси цифрової трансформації.
2.	Нестача кваліфікованих спеціалістів з кібербезпеки	В умовах зростаючого попиту на професіоналів у сфері кібербезпеки спостерігається дефіцит кваліфікованих кадрів. Згідно з дослідженням (ISC)² Cybersecurity Workforce Study, глобальна нестача фахівців у цій галузі становить 3,4 мільйона, причому 70% організацій мають незакриті вакансії. Багато держав намагаються зменшити цей дефіцит, а великі компанії, такі як Google, Microsoft і IBM, впроваджують різні ініціативи для навчання та підвищення кваліфікації людей у сфері кібербезпеки. Всесвітній економічний форум, спільно з кількома компаніями, запустив освітню онлайн-платформу для окремих осіб та організацій під назвою Cybersecurity Learning Hub. Цей проект має на меті навчання та вдосконалення навичок спеціалістів з кібербезпеки, щоб забезпечити високу якість роботи в цій сфері.
3.	Недостатня підтримка інклюзивного персоналу	Окрім дефіциту кадрів, іншим викликом для кібербезпеки є підтримка різноманітності та інклюзивності під час набору персоналу. Для залучення менш захищених груп суспільства, таких як люди з інвалідністю, необхідно розробити спеціальні ініціативи та політики. Це не лише питання цінностей, а й виклик для інновацій та продуктивності, які є ключовими факторами успіху будь-якої організації. Залучення таких груп допоможе також скоротити дефіцит кваліфікованих фахівців з кібербезпеки.
4.	Перехід на дистанційну та гібридну роботу	У зв'язку з цифровою трансформацією бізнесу, спричиненою пандемією, багато компаній зіткнулися з проблемами в безпеці корпоративного середовища. Кількість спроб атак на протокол віддаленого робочого столу (RDP) зросла на рекордні 768% у 2020 році, виявивши його як одне з найбільш уразливих місць в інфраструктурі підприємств. Тому компаніям важливо продовжувати належну підготовку та забезпечення можливостей співробітникам, які працюють віддалено, щоб уникнути потенційних ризиків і захиститися від нових атак кіберзлочинців, які постійно шукають нові недоліки в кібербезпеці корпоративних мереж.
5.	Підвищена активність у даркнеті	Зростання кримінальної активності в даркнеті в останні роки, особливо після початку пандемії, стало серйозною проблемою, що відновила актуальність досліджень у цих мережах Інтернету. Моніторинг даркнету є важливим інструментом для спеціалістів з кібербезпеки, оскільки він допомагає у запобіганні атак, розумінні стратегій шахраїв та кіберзлочинців, виявленні шкідливих інструментів, які використовуються для злому систем організацій або обману користувачів, а також для виявлення обігу корпоративних даних на чорних ринках.

6.	Нові тактики кібератак	Недавно зареєстрована активізація гібридного фішингу, який поєднує традиційний метод, що базується на електронній пошті, з фішингом, становить серйозну загрозу безпеці. Цей вид атак використовується для незаконного доступу до систем організацій та розгортання шкідливих програм, наприклад, програм-вимагачів. Під час останньої атаки потенційна жертва спочатку отримує електронний лист, наприклад, щодо продовження підписки на певну послугу. Інформація про те, що можна скасувати підписку, надається разом із контактним номером служби підтримки, зазначеним у листі. Під час дзвінка до цього номеру потенційну жертву намагаються переконати встановити шкідливу програму, яка часто може заражати інші пристрої. Водночас розвиток можливостей машинного навчання, які дозволяють створювати штучні голоси, є ще однією причиною наростаючого ризику. Спостерігається зростання атак, під час яких зловмисники використовують інструменти машинного навчання, зокрема, для імітації голосу керівника компанії у реальному часі. Це дозволяє їм переконати співробітників переказати кошти на рахунок, який, на жаль, належить зловмисникам.
7.	Зростання інтересу до криптовалюти	Зростаюча популярність криптовалют не залишилася поза увагою кіберзлочинців. Поряд з користувачами, компаніями та державними установами, які знаходять нові способи використання криптовалют, злочинці також активно освоюють цю сферу. Збільшення кількості шахрайських схем, пов'язаних з криптовалютами, свідчить про значний інтерес хакерів до цієї галузі. Виклики забезпечення безпеки у світі криптовалют регулярно стають гарячими новинами. Зловмисники часто створюють фішингові веб-сайти, імітуючи криптовалютні платформи, NFT-проекти та ігрові майданчики, з метою викрадення облікових даних користувачів, зокрема доступу до їхніх криптогаманців. Водночас криптовалютні біржі опиняються під прицілом кібергруп, що спеціалізуються на цілеспрямованих атаках. Нещодавно було зафіксовано викрадення криптовалюти на суму 625 мільйонів доларів із відеогри Axie Infinity, за яким, ймовірно, стоять хакери з групи Lazarus.
8.	Активність програм-вимагачів все ще зависока	Програми-вимагачі продовжують становити серйозний ризик, від якого організаціям необхідно ретельно захищатися. Ключові заходи включають впровадження спеціальних інструментів для протидії таким атакам, організацію ґрунтовних навчальних програм з кібербезпеки для персоналу, а також розробку планів відновлення на випадок успішного зараження. З 2020 по 2021 рік кількість атак вимагачів подвоїлася, підтверджуючи, що це залишається однією з найбільш деструктивних загроз для бізнесу.
9.	Вплив віртуального світу	Прогнози вказують, що до 2026 року кожна четверта людина в світі проводитиме щонайменше годину на день у метавсесвіті - віртуальному цифровому просторі. Це означає, що забезпечення безпеки в метавсесвіті стане важливим майбутнім викликом. Спільні віртуальні світи для взаємодії та ігор, безсумнівно, створять сприятливе середовище для численних кібератак і шахрайських схем. Крім того, в гонитві за швидким виходом на ринок, розробники інноваційних технологій часто нехтують питаннями безпеки та конфіденційності даних при створенні нових продуктів.
10.	Недостатня обізнаність користувачів	Основною проблемою, з якою стикається кібербезпека, є низький рівень обізнаності працівників щодо різних векторів кібератак та способів їх розпізнавання. Саме тому персонал вважається найбільш вразливою ланкою в системі захисту будь-якої організації. Проте за умови належного навчання та підвищення рівня поінформованості про сучасні кіберзагрози, співробітники можуть стати першою лінією кіберзахисту. Ознайомитися з найпоширенішими онлайн-ризиками та рекомендаціями щодо захисту від них можна з доступних інформаційних матеріалів та навчальних ресурсів з кібербезпеки.

Створено автором на основі [4].

pocatku-vijni-rosijski-hakeri-zdijsnuut-po-45-tisaci-kiberatak-soroku-sbu.html

3. Звіт національної поліції України про результати роботи у 2023 році. *Нац. поліція України*. 12 с. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Dialnist/Richni_zvity/zvit_NPU_2023.pdf.

4. 10 викликів кібербезпеки: експерти розповіли, до чого готуватися користувачам та компаніям. *УНІАН*. URL: https://www.unian.ua/science/10-viklikiv-kiberbezpeki-eksperti-rozpovili-do-chogo-gotuvatisya-koristuvacham-ta-kompaniyam-12033828.html

CYBERSECURITY CHALLENGES FOR LAW ENFORCEMENT AGENCIES IN THE DIGITAL AGE

In today's world, where digital technologies are rapidly evolving and penetrating all spheres of life, law enforcement agencies face new challenges in the field of cybersecurity. It has been determined that criminals are increasingly using cyberspace to commit illegal acts, which jeopardizes the security of the state, business and citizens. Therefore, law enforcement agencies need to adapt to these changes and develop effective strategies to combat cybercrime.

The problem of cybersecurity and the challenges posed by cybercrime to law enforcement agencies are the subject of active research in the modern scientific literature. Many studies are devoted to analyzing cybersecurity threats and developing strategies to overcome them. However, there is a need for further research to develop new approaches and strategies to combat cybercrime in the context of rapid technological development.

The article studies the current problems faced by law enforcement agencies in connection with the growth of cyber threats in the modern digital world. The author analyzes a wide range of challenges faced by law enforcement agencies in the field of cybersecurity, such as cyberattacks, cyberespionage, cyberterrorism, etc. The article also discusses strategies and methods of combating cyber threats, including improving technical means of protection, staff training and the development of international cooperation in the field of cybersecurity. Through systematic analysis and coverage of current trends in this area, this line of research contributes to a better understanding of the complexities and prospects for the development of cybersecurity in the context of law enforcement.

As a result of the work, it was determined that it is important to conduct a detailed study of the current state of cybersecurity of Ukraine in the context of military conflict and to understand the need to protect cyberspace under the threat of war. The ability of a country to effectively protect its information assets during military conflicts is becoming a crucial factor for ensuring national security and stimulating economic development.

Keywords: cybersecurity, cybercrime, law enforcement agencies, martial law, national security.