УДК 004.056
DOI https://doi.org/10.32782/2408-9257-2024-6-25

Шевчук М. О.,
кандидат юридичних наук,
докторант кафедри конституційного, адміністративного та фінансового права
Хмельницького університету управління та права імені Леоніда Юзькова
https://orcid.org/0000-0001-7549-6344

СУЧАСНІ ВИКЛИКИ І ЗАГРОЗИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

MODERN CHALLENGES AND THREATS IN THE FIELD OF STATE INFORMATION SECURITY

У цій статті розглядаються сучасні виклики та загрози національній інформаційній безпеці в контексті цифрової трансформації та глобалізації. Обговорюються ключові аспекти кіберзлочинності, такі як фішинг, DDoS-атаки, злом баз даних, цифрове шпигунство і крадіжка конфіденційної інформації. Особлива увага приділяється інформаційній війні, включно з пропагандою, поширенням фальшивих новин і маніпулюванням громадською думкою. Автор виокремлює проблему вразливості критичних інформаційних інфраструктур, особливо в енергетичному, транспортному та фінансовому секторах, і підкреслює важливість їхнього захисту. Автор акцентує увагу на розвитку технологій штучного інтелекту, які можуть бути використані як як інструменти атаки, так і як ефективні засоби нейтралізації загроз. Автор обговорює сучасні підходи до протидії цим викликам, такі як зміцнення нормативно-правової бази, впровадження інноваційних технологій кіберзахисту, створення систем раннього попередження та розробка адаптивних стратегій реагування. Зокрема, важливо формувати культуру інформаційної безпеки серед громадян, зокрема підвищувати медіаграмотність, навчати основ безпечного використання цифрових ресурсів і виховувати відповідальне ставлення до захисту інформації. У статті підкреслюється, що забезпечення національної інформаційної безпеки вимагає комплексного підходу, що охоплює технічні, правові та соціальні аспекти. Висновки статті акцентують увагу на об'єднанні зусиль держави, бізнесу та суспільства для створення надійної системи захисту інформаційного простору. Це дасть змогу мінімізувати ризики, підвищити стійкість інформаційної інфраструктури та забезпечити стабільність цифрової економіки.

Ключові слова: *кіберзлочинність, цифрове шпигунство, інформаційна війна, уразливість критичної інформаційної інфраструктури, штучний інтелект, фейки та маніпуляції, технології кіберзахисту, культура інформаційної безпеки.*

This article examines modern challenges and threats to national information security in the context of digital transformation and globalization. Key aspects of cybercrime, such as phishing, DDoS attacks, database breaches, digital espionage, and theft of confidential information, are discussed. Particular attention is paid to information warfare, including propaganda, the spread of fake news, and manipulation of public opinion. The author highlights the vulnerability of critical information infrastructures, especially in the energy, transportation, and financial sectors, emphasizing the importance of their protection. The focus is placed on the development of artificial intelligence technologies, which can be utilized both as tools for attacks and as effective means to neutralize threats. The author discusses modern approaches to counteracting these challenges, such as strengthening the legal framework, implementing innovative cybersecurity technologies, creating early warning systems, and developing adaptive response strategies. The importance of fostering a culture of information security among citizens is underscored, particularly through enhancing media literacy, teaching the basics of safe use of digital resources, and promoting a responsible attitude toward information protection. The article emphasizes that ensuring national information security requires a comprehensive approach that encompasses technical, legal, and social aspects. The conclusions highlight the need for collaboration between the state, business, and society to establish a reliable system for protecting the information space. This approach will minimize risks, enhance the resilience of information infrastructure, and ensure the stability of the digital economy.

Key words: *cybercrime, digital espionage, information warfare, vulnerability of critical information infrastructure, artificial intelligence, fakes and manipulation, cybersecurity technologies, information security culture.*

Постановка проблеми. Інформаційна безпека – одна зі складових національної безпеки країни, що охоплює всі сфери суспільного життя, особливо в умовах цифрової трансформації. Розвиток інформаційних технологій відкриває нові можливості для економічного зрос-

тання, ефективності управління та зручності громадян. Однак водночас він створює й нові виклики, які потребують належної уваги та реагування. Важливість теми інформаційної безпеки зумовлена зростанням кількості кіберзагроз, які стають дедалі складнішими, а їхній вплив – глобальним.

Аналіз останніх досліджень. Дослідження сучасних викликів і загроз у сфері інформаційної безпеки держави висвітлені у працях як вітчизняних, так і зарубіжних науковців, серед яких В. Виздрик, О. Мельник, М.Т. Гаврильців, І.І. Залєвська, Г.І. Удренас, У. Ільницька, О.А. Ніщименко, О. Панченко, Н.С. Уханова та інші. Однак аналіз цієї проблеми часом має фрагментарний характер, концентруючись на окремих аспектах інформаційної безпеки, таких як кіберзлочинність, інформаційна війна і правові аспекти захисту інформаційного простору. Багато авторів вважають за краще описувати конкретні загрози, такі як фішинг, DDoS-атаки або пропаганда, не беручи до уваги їхню взаємозалежність і вплив на критичну інфраструктуру. Водночас на сьогодні не існує комплексного дослідження, яке охоплювало б усі важливі аспекти сучасних викликів національній інформаційній безпеці, включно з технічними, правовими, соціальними та культурними чинниками. Необхідність такого дослідження зумовлена зростаючою складністю загроз, що вимагає комплексного підходу до їхнього аналізу та заходів протидії.

Метою цієї статті є аналіз основних викликів і загроз інформаційній безпеці держави, що виникають у сучасних умовах. Особлива увага приділяється їхній характеристиці, оцінці впливу на національну безпеку та суспільство, а також розгляду можливих шляхів мінімізації їхнього негативного впливу.

Виклад основного матеріалу. Глобалізація, що стала невід'ємною рисою сучасного світу, докорінно змінює підхід до забезпечення національної інформаційної безпеки. Розвиток цифрових технологій і поширення глобальних мереж створюють умови для ефективного обміну інформацією, але водночас породжують численні загрози. Зростання кіберзагроз – одна з найсерйозніших проблем, з якими стикаються держави в сучасних умовах.

Кіберзлочинність, діяльність хакерських груп, використання шкідливих програм і поширення фішингових атак стають дедалі поширенішими. Це пов'язано не тільки зі збільшенням обсягу даних, що зберігаються в цифровому вигляді, а й з ускладненням атак, спрямованих на державні відомства, приватні компанії та критично важливу інфраструктуру. Держави стають потенційними об'єктами атак, спрямованих не тільки на нанесення економічного збитку, а й на дестабілізацію політичної ситуації [6, с. 59].

У зв'язку з цим важливість ефективного захисту інформаційної безпеки значно зросла. Основна проблема полягає в тому, що механізми захисту відстають від темпів розвитку загроз. Тому державам необхідно постійно оновлювати свої стратегії, впроваджувати інноваційні технології та запобігати глобальним ризикам за допомогою міжнародного співробітництва. Попри свої позитивні сторони, глобалізація створює великий простір для нових викликів, які потребують швидкої адаптації та адекватного реагування.

Розвиток технологій штучного інтелекту – одне з найважливіших досягнень сучасності, що зачіпає всі сфери життя, зокрема й інформаційну безпеку. Штучний інтелект відкриває нові можливості для автоматизації процесів, обробки даних і створення передових систем кіберзахисту. Водночас ця технологія може бути використана зловмисниками як потужний інструмент для проведення атак, що значно ускладнює завдання із захисту інформаційної інфраструктури країни.

Штучний інтелект може автоматизувати кіберзагрози і зробити їх складнішими і масштабнішими. Наприклад, хакери можуть використовувати алгоритми машинного навчання для адаптації систем безпеки, виявлення їхніх вразливостей і створення шкідливого програмного забезпечення, що обходить традиційні методи захисту. Крім того, штучний інтелект може аналізувати поведінку користувачів і виявляти найбільш вразливі елементи системи, що дає змогу проводити цілеспрямовані атаки.

Особливу небезпеку становлять технології глибокого підроблення на основі штучного інтелекту, які можна використовувати для створення реалістичних підробок відео та аудіозаписів з метою поширення дезінформації,

маніпулювання громадською думкою та дискредитації політичних лідерів. Вони можуть бути використані для створення реалістичних підробок зображень і звуку з метою поширення дезінформації, маніпулювання громадською думкою та дискредитації політичних лідерів. Це підриває довіру до інформації і може мати серйозні наслідки [1, с. 197].

Сучасні технології дозволяють зловмисникам отримувати доступ до конфіденційних даних різними способами, починаючи від фішингових атак і закінчуючи проникненням у захищені системи за допомогою складних кіберзасобів. Ця проблема особливо актуальна для державних установ, військових відомств і великих корпорацій, що працюють зі стратегічно важливою інформацією.

Найчастіше цифрове шпигунство здійснюється за допомогою шкідливого програмного забезпечення, яке таємно проникає в комп'ютерні системи і збирає дані. Також поширені атаки на хмарні сервіси, де зберігаються великі обсяги конфіденційної інформації. Уразливими залишаються і мобільні пристрої, що використовуються для передачі службових даних. Цифрове шпигунство – це не тільки проблема кібербезпеки, а й проблема національної безпеки, оскільки зловмисники часто діють за іноземного сприяння.

Крадіжка конфіденційної інформації може мати катастрофічні наслідки. Це може призвести до витоку державних секретів, зриву дипломатичних переговорів, економічних втрат або навіть ослаблення обороноздатності країни. Крім того, подібні інциденти можуть завдати непоправної шкоди репутації держави або організації, яка не забезпечила належний рівень захисту.

Щоб протистояти загрозі цифрового шпигунства, необхідно впроваджувати новітні технології шифрування даних, посилювати контроль доступу до інформації та регулярно проводити аудит кібербезпеки. Також важливо проводити навчання співробітників, які працюють із конфіденційними даними, і мінімізувати людський фактор, який часто стає причиною успішних атак. Ефективний захист конфіденційної інформації вимагає комплексного підходу, що включає як технічні рішення, так і політичні заходи на національному рівні.

Кіберзлочинність проявляється у вигляді різних форм злочинної діяльності, пов'язаної з використанням інформаційних технологій. Одним із найпоширеніших методів є фішинг, метою якого є ошуканство користувачів з метою отримання особистих даних, паролів або фінансової інформації. Фішингові атаки здійснюються через електронні листи, повідомлення в соціальних мережах і сайти, що видають себе за легітимні ресурси. Успіх таких атак часто пояснюється недостатньою обізнаністю користувачів і неадекватною безпекою на рівні компанії або організації.

Іншою серйозною загрозою є DDoS-атаки (розподілені атаки типу «відмова в обслуговуванні»), які перевантажують сервери і блокують доступ до критично важливих ресурсів. Такі атаки використовуються для шантажу, організаційної нестабільності та навіть соціальної паніки. DDoS-атаки особливо небезпечні для критично важливих об'єктів інфраструктури, таких як банківські системи, енергетичні мережі та урядові портали, і їхній успіх може мати далекосяжні наслідки [4, с. 31].

Злом баз даних – ще одна поширена форма кіберзлочинності. Зловмисники отримують доступ до величезних обсягів інформації, включно з персональними даними, фінансовими звітами та комерційними таємницями. Вкрадені дані часто використовуються для шахрайства, здирництва та продажу на чорному ринку. Уразливості баз даних зазвичай спричинені недотриманням кібергігієни, застарілим програмним забезпеченням і слабкими паролями.

Боротьба з кіберзлочинністю вимагає комплексного підходу, що включає технічні засоби захисту, правові норми та інформованість користувачів. Регулярне оновлення програмного забезпечення, впровадження багаторівневої автентифікації та навчання персоналу – елементи зниження ризиків, пов'язаних із цим видом загроз.

Інформаційна війна впливає на політичну стабільність, соціальну згуртованість і національну безпеку. Одним з основних інструментів такої війни є пропаганда, мета якої – створити викривлене уявлення про реальність, маніпулювати суспільними настроями та формувати наратив на користь агресора. Про-

пагандистські кампанії використовують різні медіаплатформи для поширення своєї ідеології, зниження довіри до офіційних джерел і розколу суспільства.

Фальшиві новини, що набули поширення в цифрову епоху, також становлять загрозу. Такі новинні агентства часто видають себе за надійні джерела, але їхня мета – поширення дезінформації. Фальшиві новини можуть створюватися і поширюватися окремими особами, організованими групами або іноземними урядами. Фальшиві новини сіють паніку, дискредитують політичних лідерів та інститути і створюють хибне уявлення про світові події.

Маніпулювання громадською думкою – ще один аспект інформаційної війни, який має довгострокові наслідки. Використовуючи соціальні мережі та інші цифрові платформи, зловмисники створюють контент, спрямований на поляризацію суспільства, загострення конфліктів і підрив соціальної гармонії. Подібні маніпуляції включають у себе використання ботів, що створюють видимість масової підтримки певної ідеології, і таргетовану рекламу, яка використовує емоційні тригери громадян [7, с. 159].

Протидія інформаційній війні вимагає активної участі державних органів, ЗМІ, неурядових організацій та технологічних компаній. Важливо підвищувати медіаграмотність населення, створювати механізми перевірки фактів і посилювати регулювання соціальних мереж. Лише координуючи зусилля на різних рівнях, можна ефективно протистояти пропаганді, фальшивим новинам і маніпуляціям, які загрожують безпеці та стабільності сучасних держав.

Системи, що забезпечують функціонування енергетики, транспорту, фінансових установ та інших ключових галузей, стають головною мішенню для кіберзлочинців і ворожих держав. Успішні атаки на ці об’єкти можуть мати катастрофічні наслідки, включно з порушенням роботи енергетичних мереж, транспортних систем, банківських операцій та економічною нестабільністю.

Енергетична інфраструктура особливо вразлива, оскільки вона значною мірою автоматизована і спирається на мережеві технології. Кіберзагрози, спрямовані на електростанції та нафто- і газопроводи, можуть вивести з ладу системи управління, що призведе до перебоїв в енергопостачанні та серйозних економічних втрат. Зловмисники можуть використовувати шкідливе програмне забезпечення для проникнення в інфраструктуру, що може мати фізичний вплив на промислові системи.

Транспортні системи також піддаються нападам, оскільки вони відіграють найважливішу роль у забезпеченні безперебійного функціонування держави. Уразливості в повітряних, залізничних і дорожніх системах можуть загрожувати безпеці пасажирів і вантажів. Атаки на системи управління транспортом можуть порушити логістичні процеси і паралізувати роботу найважливіших вузлів. Це особливо небезпечно для великих міст, де транспортна інфраструктура відіграє важливу роль у міському житті.

Фінансові системи – ще одна вразлива ланка критичної інформаційної інфраструктури. Злам банківських систем, крадіжка даних клієнтів або маніпуляції з фондовими біржами можуть призвести до значних економічних втрат, підірвати довіру до фінансових інституцій і викликати паніку серед населення. Такі атаки зазвичай здійснюються з метою отримання фінансової вигоди або дестабілізації економічної ситуації в країні.

Щоб знизити вразливість критичної інформаційної інфраструктури, необхідно реалізувати комплексні заходи захисту, включно з регулярним аудитом систем, модернізацією обладнання, навчанням персоналу та впровадженням передових технологій кібербезпеки.

Сучасні виклики вимагають від держав розробки та впровадження ефективних правових механізмів, здатних регулювати діяльність у цифровому середовищі, захищати критичну інфраструктуру та гарантувати права громадян на недоторканність приватного життя і безпеку даних. Розробка комплексної правової бази включає в себе визначення відповідальності за кіберзлочини, впровадження стандартів кіберзахисту та забезпечення механізмів міжнародного співробітництва для боротьби з глобальними загрозами.

Одним із важливих аспектів є гармонізація національних законів із міжнародними нормами та стандартами. Оскільки більшість загроз

мають транснаціональний характер, це допомагає забезпечити ефективну співпрацю з іншими країнами в боротьбі з кіберзлочинністю. Наприклад, участь у Будапештській конвенції про кіберзлочинність полегшує обмін інформацією між національними правоохоронними органами та спрощує процедури розслідування кіберзлочинів.

Крім того, правова база має враховувати розвиток нових технологій і передбачати регулювання їхнього використання. Наприклад, безпека технологій штучного інтелекту, великих даних і блокчейну має бути чітко прописана в законі, щоб уникнути можливих зловживань і ризиків. У цьому контексті також важливо звернути увагу на права користувачів, особливо щодо зберігання та обробки персональних даних.

Запровадження ефективних санкцій за порушення правил інформаційної безпеки також є необхідною умовою ефективного захисту. Необхідно чітко визначити відповідальність для компаній, організацій та приватних осіб, які ігнорують вимоги безпеки або навмисно діють у такий спосіб, що загрожують інформаційній інфраструктурі. Водночас важливо враховувати баланс між безпекою та свободою в цифровому середовищі, щоб не обмежувати демократичні права та свободи громадян.

У сучасному світі технології відіграють ключову роль у захисті інформаційних систем від атак і витоків даних. Впровадження передових рішень у сфері кібербезпеки дає змогу не тільки виявляти та реагувати на загрози, а й запобігати їм.

Одним із важливих напрямів є використання технологій штучного інтелекту для аналізу кіберзагроз. Алгоритми машинного навчання здатні швидко обробляти великі обсяги даних, виявляти підозрілу активність у мережі та прогнозувати можливі атаки. Це дає змогу створювати системи проактивного захисту, здатні реагувати на загрози в режимі реального часу і мінімізувати їхні наслідки.

Ще один важливий аспект – розробка програмного забезпечення для захисту інформаційних систем. Сучасні антивірусні програми, системи виявлення вторгнень і засоби шифрування даних постійно вдосконалюються, щоб протистояти новим формам загроз. Особливе значення має впровадження технологій багатофакторної автентифікації та парольного захисту, що забезпечують надійний контроль доступу до критично важливих систем.

Також важливо розвивати технології захисту хмарних сервісів, які широко використовуються в бізнесі та державному секторі. Засоби моніторингу активності, контролю доступу та шифрування в хмарних середовищах дають змогу ефективно захистити дані від несанкціонованого доступу та витоку.

Важливими елементами технічного захисту є також регулярна модернізація інфраструктури та впровадження сучасного обладнання. Рівень безпеки системи може бути значно підвищений за рахунок використання захищених мережевих протоколів, ізольованих середовищ для тестування програмного забезпечення та інших інноваційних рішень [3, с. 23].

Формування культури інформаційної безпеки в суспільстві – важливий чинник забезпечення стабільності перед обличчям сучасних кіберзагроз. Культура безпеки визначає не тільки рівень технічного захисту, а й усвідомлення суспільством необхідності дотримання правил безпеки в цифровому середовищі. Вона включає в себе набір знань, навичок і моделей поведінки, які допомагають людям розуміти потенційні загрози та реагувати на них.

Одним із важливих аспектів формування такої культури є підвищення рівня медіаграмотності громадян. Це означає не лише вміння користуватися цифровими технологіями, а й здатність критично ставитися до одержуваної інформації, розрізняти надійні та ненадійні джерела інформації та розуміти, як захистити свої особисті дані. У суспільстві, де більша частина інформації надходить з Інтернету і соціальних мереж, важливо, щоб люди володіли достатніми знаннями про те, як захистити себе від фальшивих новин, кібератак і маніпулювання інформацією [2, с. 202].

Освітні програми, включно з навчанням інформаційної безпеки, мають бути інтегровані на всіх рівнях, від шкіл до корпоративного навчання співробітників. Інформаційна безпека – це не тільки технічна тема для ІТ-фахівців, важливо зробити її доступною для широкої аудиторії, щоб у кожного була можливість застосовувати основні принципи безпеки в повсякденному житті.

Крім того, культура інформаційної безпеки включає в себе й етичні аспекти використання цифрових технологій. Йдеться не лише про дотримання закону, а й про розвиток відповідальності за власну поведінку в мережі. Користувачі мають розуміти важливість захисту конфіденційної інформації, поважати права інших людей і не створювати загроз безпеці через власну необережність чи недбалість.

Інформаційна безпека має бути частиною національної політики, а також частиною корпоративної стратегії. Культура безпеки, сформована на рівні держав і великих організацій, допоможе забезпечити ефективну взаємодію в цифровій економіці та протистояти таким загрозам, як кіберзлочинність та онлайн-пропаганда.

Формування культури інформаційної безпеки в суспільстві – важливий чинник забезпечення стабільності перед обличчям сучасних кіберзагроз. Культура безпеки визначає не тільки рівень технічного захисту, а й усвідомлення суспільством необхідності дотримання правил безпеки в цифровому середовищі. Вона включає в себе набір знань, навичок і моделей поведінки, які допомагають людям розуміти потенційні загрози та реагувати на них.

Одним із важливих аспектів формування такої культури є підвищення рівня медіаграмотності громадян. Це означає не лише вміння користуватися цифровими технологіями, а й здатність критично ставитися до одержуваної інформації, розрізняти надійні та ненадійні джерела інформації та розуміти, як захистити свої особисті дані. У суспільстві, де більша частина інформації надходить з Інтернету та соціальних мереж, важливо, щоб люди володіли достатніми знаннями про те, як захистити себе від фальшивих новин, кібератак і маніпулювання інформацією [5, с. 19].

Освітні програми, включно з навчанням інформаційної безпеки, мають бути інтегровані на всіх рівнях, від шкіл до корпоративного навчання співробітників. Інформаційна безпека – це не тільки технічна тема для ІТ-фахівців, а й важливо зробити її доступною для широкої аудиторії, щоб у кожного була можливість застосовувати основні принципи безпеки в повсякденному житті.

Висновки. Отже, інформаційна безпека є ключовим елементом національної безпеки будь-якої держави, а її ефективний захист набуває вирішального значення в умовах стрімкого розвитку цифрових технологій. Сучасні виклики та загрози в галузі інформаційної безпеки, такі як кіберзлочинність, цифрове шпигунство, інформаційна війна та атаки на критичну інфраструктуру, потребують комплексного підходу для їх нейтралізації. Оскільки ці загрози можуть серйозно вплинути на економічну, політичну та соціальну стабільність, протидія їм є пріоритетним завданням для урядів, бізнесу та суспільства в цілому.

Розробка та впровадження ефективних технологій кіберзахисту – необхідна умова для захисту інформаційної інфраструктури країни від зовнішніх і внутрішніх загроз. Інвестиції в інноваційні технології, включно зі штучним інтелектом та інструментами для боротьби з кіберзлочинністю, допоможуть створити більш стійку систему захисту і знизити ймовірність успішних атак. Водночас важливим елементом є зміцнення нормативно-правової бази для розв'язання нових завдань цифрової трансформації та запровадження відповідних санкцій за порушення інформаційної безпеки.

Слід також наголосити на важливості культури інформаційної безпеки, яка має формуватися в суспільстві за допомогою освітніх програм, медіаграмотності та розвитку почуття громадянської відповідальності за забезпечення цифрової безпеки. Важливо, щоб усі члени суспільства усвідомлювали свою роль у загальному процесі захисту інформаційних ресурсів і вміли застосовувати основні принципи безпеки в цифровому середовищі.

ЛІТЕРАТУРА:

1. Виздрик В., Мельник О. Інформаційна безпека в Україні. *Grail of Science*. 2023. № 24. С. 196–202.

2. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200–203.

3. Залєвська І.І., Удренас Г.І. Інформаційна безпека в Україні в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1. С. 20–26.

4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2019. № 1. Вип. 2. С. 27–32.

5. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2018. № 1. С. 17–23.

6. Панченко О. Інформаційна безпека держави як елемент соціокультури. *Аспекти публічного управління*. 2020. № 1. С. 58–67.

7. Уханова Н.С. Правова культура молоді в Україні. *Інформація і право.* 2019. № 2. С. 156–166.