УДК 004.056
DOI https://doi.org/10.24144/2307-3322.2025.90.5.58

ІНФОРМАЦІЙНА БЕЗПЕКА: НОВІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАХИСТУ

Колб С.О.,
кандидат юридичних наук, доцент,
доцент кафедри права
Волинського інституту імені В'ячеслава Липинського
ПрАТ «ВНЗ МАУП»,
адвокат АО «Бона Фіде»
e-mail: Kolbserhii86@gmail.com

Пирога М.І.,
студент 1-го курсу другого (магістерського) рівня вищої освіти,
юридичного факультету
Ужгородського національного університету
e-mail: maksa7@meta.ua

Колб С.О., Пирога М.І. Інформаційна безпека: нові виклики та стратегії захисту.

Вказується, інформаційна безпека на сучасному етапі становить одну з найбільш критичних проблем як для індивідуальних користувачів, так і для корпоративних структур у світовому масштабі.

Інформаційна безпека стала невід'ємною частиною сучасного цифрового середовища, адже обробка, зберігання та передача величезних обсягів даних відбуваються щодня через різноманітні платформи. З розвитком технологій зростають не лише можливості для зручності та ефективності, а й нові загрози, які супроводжують цей прогрес. У 2025 році ми спостерігаємо значне збільшення складності та різноманітності кіберзагроз, що ставлять під сумнів ефективність традиційних методів захисту. Злочинці дедалі більше застосовують новітні технології, зокрема штучний інтелект, для створення складних атак, що дозволяє обирати нові способи проникнення в систему особистих даних. Водночас розвиток таких інновацій, як Інтернет речей та 5G, додає додаткових вразливих точок у цифровій інфраструктурі. Наразі важливо не лише адаптувати існуючі стратегії захисту, але й розробляти нові підходи, які здатні забезпечити оперативне реагування на кіберзагрози. Особливого значення набуває створення багаторівневих систем захисту, впровадження інтелектуального моніторингу та виявлення аномалій у режимі реального часу. Тому важливо вдосконалювати системи автентифікації та контролю доступу з урахуванням динаміки розвитку загроз. Окрему увагу слід приділити людському фактору – підвищенню цифрової грамотності користувачів та формуванню культури кібергігієни, що є критичними умовами побудови стійкої безпекової системи. Таким чином, сучасна інформаційна безпека потребує комплексного підходу, який охоплює не лише технічні засоби, але й організаційні механізми, законодавче регулювання та освітні ініціативи. У статті окреслено ключові тенденції та напрями трансформації стратегій інформаційного захисту у відповідь на виклики 2025 року. Значення проведеного аналізу полягає в узагальненні актуальних підходів до формування національної інформаційної політики. Отримані результати можуть стати підґрунтям для практичного впровадження інноваційних рішень у сфері кібербезпеки.

Ключові слова: Інформаційна безпека; технології; захист даних; новітні технології; штучний інтелект; особиста інформація.

Kolb S.O., Pyroha M.I. Information security: new challenges and protection strategies.

It is indicated that information security at the current stage is one of the most critical problems for both individual users and corporate structures on a global scale.

Information security has become an integral part of the modern digital environment, as huge amounts of data are processed, stored and transmitted daily across a variety of platforms. With the development of technology, not only the opportunities for convenience and efficiency are growing, but also the new threats that accompany this progress. In 2025, we will see a significant increase in the complexity and diversity of cyber threats, which calls into question the effectiveness of traditional protection methods. Criminals are increasingly using the latest technologies, including artificial intelligence, to create sophisticated attacks, which allows them to choose new ways to penetrate the personal data system. At the same time, the development of innovations such as the Internet of Things and 5G adds additional vulnerabilities to the digital infrastructure. It is now important not only to adapt existing protection strategies, but also to develop new approaches that can provide a prompt response to cyber threats. The creation of multi-layered protection systems, the implementation of intelligent monitoring and the detection of anomalies in real time are of particular importance. At the same time, it is important to improve authentication and access control systems taking into account the dynamics of threat development. Special attention should be paid to the human factor - increasing the digital literacy of users and forming a culture of cyber hygiene are critical conditions for building a sustainable security system. Thus, modern information security requires a comprehensive approach that encompasses not only technical means, but also organizational mechanisms, legislative regulation and educational initiatives. The article outlines key trends and directions for the transformation of information protection strategies in response to the challenges of 2025. The significance of the analysis is to generalize current approaches to the formation of national information policy. The results obtained can become the basis for the practical implementation of innovative solutions in the field of cybersecurity.

Key words: Information security; technology; data protection; new technologies; artificial intelligence; personal information.

Постановка проблеми. Інформаційна безпека сьогодні є однією з головних проблем як для окремих користувачів, так і для організацій на глобальному рівні. У світі, де майже кожен аспект нашого життя так чи інакше пов'язаний із цифровими технологіями, захист персональних та корпоративних даних стає пріоритетом. Розвиток новітніх технологій, таких як Інтернет речей, штучний інтелект та хмарні обчислення, відкриває нові можливості, але водночас і нові виклики для безпеки.

Основною проблемою є швидке ускладнення кіберзагроз. Зловмисники постійно вдосконалюють свої методи атаки, використовуючи новітні технології для створення складних і важко виявлених загроз. Традиційні системи захисту, такі як антивіруси чи фаєрволи, стають менш ефективними в умовах постійних змін у цифровому середовищі. Кібератаки стають все більш різноманітними та професійними, що змушує організації адаптувати свої стратегії безпеки, інтегруючи нові методи виявлення та реагування на загрози.

Ще однією серйозною проблемою є зростаюча кількість пристроїв, підключених до Інтернету – від смартфонів до «розумних» домашніх пристроїв. Всі вони потенційно можуть бути вразливими до атак. Більшість таких пристроїв мають низький рівень безпеки або взагалі не оснащені ефективними механізмами захисту, що дозволяє зловмисникам отримувати доступ до приватних даних або навіть здійснювати атаки через слабкі ланки в мережі.

Не менш важливою є проблема людського фактору. Незважаючи на високий рівень технологічного розвитку, більшість інцидентів у сфері кібербезпеки трапляються через необережність або недооцінку загроз з боку користувачів. Використання слабких паролів, необережність при відкритті підозрілих листів чи переході за невідомими посиланнями створює вразливі точки, через які можуть бути здійснені атаки.

Стан опрацювання цієї проблематики. Серед провідних дослідників, які зробили вагомий внесок у розвиток теорії та практики інформаційної безпеки, слід відзначити таких вітчизняних фахівців як: О.І. Баранов, В.В. Брижко, С.А. Макєєв, а також зарубіжних науковців – Брюса Шнайєра, Ю. Сільвера, Кевіна Митника. Їхні роботи присвячено аналізу сучасних загроз, моделюванню кіберінцидентів, розробці стратегій захисту.

Метою статті є аналіз сучасних викликів у сфері інформаційної безпеки та розгляд ефективних стратегій захисту даних в умовах швидко змінюваного цифрового середовища. У статті будуть досліджені новітні тенденції в розвитку кіберзагроз, а також можливі методи протидії їм, зокрема шляхом упровадження інноваційних технологій, удосконалення існуючих систем безпеки

та навчання користувачів. Зокрема, увага буде зосереджена на питаннях, пов'язаних із захистом персональних та корпоративних даних, боротьбою з новими формами кібератак і забезпеченням цілісності інформаційних систем у глобальному масштабі.

Виклад основного матеріалу. Одним із головних викликів, що постають перед експертами з інформаційної безпеки, є еволюція кіберзлочинності. Злочинці все частіше застосовують штучний інтелект та машинне навчання для створення складних, майже непомітних атак. Це дозволяє їм обходити традиційні засоби захисту, що базуються на сигнатурах або шаблонах [1]. Розвиток таких технологій також створює нові способи фішингу, в тому числі через голосові помилки або підроблені відео (deepfake), що ускладнює ідентифікацію злочинців. Інший важливий аспект – це розповсюдження Інтернету речей (IoT). Пристрої, що взаємодіють між собою, часто не мають достатньо захищених каналів для передачі даних або достатньої аутентифікації, що відкриває нові можливості для атак. В умовах розширеного використання 5G зв'язку та масового підключення різноманітних пристроїв ці вразливості можуть стати ще більш критичними [2]. Крім того, не можна забувати про збільшення обсягів і складності державних атак на інформаційні системи. Багато країн уже активно використовують кіберпростір для політичного та економічного впливу, що створює серйозні загрози для національної безпеки.

Щоб ефективно протистояти новим загрозам, компаніям та організаціям необхідно використовувати більш комплексні підходи до інформаційної безпеки. Однією з таких стратегій є впровадження багаторівневих систем захисту. Замість того, щоб покладатися на один метод (наприклад, антивірусні програми), необхідно інтегрувати цілу низку інструментів – від фаєрволів до систем виявлення аномалій у мережах, що дозволяє реагувати на нові загрози в реальному часі. Штучний інтелект і машинне навчання можуть не тільки допомагати зловмисникам, але й стати важливими союзниками в боротьбі з кіберзлочинністю [3]. Вони можуть використовуватися для автоматичного виявлення аномалій у великих масивах даних, що дозволяє своєчасно виявляти потенційні загрози ще до того, як вони стануть реальними проблемами. Особливу увагу необхідно приділяти захисту персональних даних [1]. Оскільки конфіденційність стає все важливішою, організації повинні активно впроваджувати принципи «нульового доступу» до даних – це означає, що навіть співробітники компанії повинні мати доступ лише до тієї інформації, яка їм дійсно необхідна.

Не менш важливим є навчання та підвищення обізнаності серед користувачів. Враховуючи, що більшість кіберінцидентів починається саме з людського фактору (наприклад, перехід на фейковий сайт або використання ненадійного паролю), постійне навчання співробітників з інформаційної безпеки стає важливим елементом стратегії.

Інформаційна безпека 2025 року вимагатиме від держав, компаній та індивідуальних користувачів постійної адаптації до нових умов та загроз. Технології не стоятимуть на місці, і, як показує досвід попередніх років, постійне вдосконалення стратегій захисту є необхідною умовою для забезпечення безпеки в цифровому світі [4]. Тому, крім технічних рішень, успіх залежатиме від готовності до співпраці, навчання та безперервного моніторингу загроз. В епоху цифрової трансформації тільки гнучкість та інноваційність можуть стати запорукою успішної боротьби з кіберзлочинністю.

Важливо зазначити, що разом з технічними інструментами вирішальне значення має розвиток нормативно-правової бази у сфері кібербезпеки. Регуляторні органи повинні оновлювати існуючі стандарти безпеки відповідно до новітніх викликів, особливо в контексті транснаціональних загроз, що не обмежуються державними кордонами. Відсутність узгоджених міжнародних механізмів реагування на кіберінциденти ускладнює ефективну співпрацю між країнами, що також створює прогалини в глобальному захисті цифрового простору. Зростає потреба у створенні спеціалізованих аналітичних центрів з реагування на інциденти (CSIRT), які могли б здійснювати оперативний моніторинг, аналіз загроз і координацію дій між приватним та державним секторами [3]. Досвід розвинених країн свідчить про ефективність таких структур у попередженні атак, які здатні спричинити масштабні наслідки для критичної інфраструктури.

Особливої уваги заслуговує проблема довіри до цифрових систем. Використання новітніх технологій, зокрема таких як блокчейн, біометричних засобів автентифікації та криптографічного захисту, дає можливість підвищити прозорість, надійність і стійкість інформаційних процесів. Проте їхнє запровадження потребує значних ресурсів, чіткого планування та підготовки персоналу. Крім того, з огляду на стрімку цифрову трансформацію, слід приділяти увагу кіберетичному вихованню молоді. Формування цифрової культури безпеки з раннього віку сприяє зниженню

ризиків зловживань і сприяє більш відповідальному ставленню до інформації [1]. Освітні програми з кібербезпеки мають стати обов'язковою частиною навчання в університетах технічного та гуманітарного профілів. У цьому контексті забезпечення кібербезпеки постає не лише як технічне чи політичне завдання, а як глобальна соціальна відповідальність. Лише через поєднання зусиль держав, приватного сектора, наукової спільноти та громадянського суспільства можна сформувати стійку цифрову екосистему, готову до протидії загрозам майбутнього.

В умовах безперервного технологічного прогресу все більшої актуальності набуває концепція «превентивної кібербезпеки», яка передбачає не лише реагування на вже виявлені загрози, а й проактивне виявлення потенційних векторів атак ще до їх реалізації. Такий підхід ґрунтується на аналізі поведінкових шаблонів у цифрових мережах, симуляції можливих сценаріїв зловживань і постійному вдосконаленні захисних механізмів. Ключовим фактором ефективності таких систем є здатність до самоадаптації – механізмів, які вчаться на основі накопиченого досвіду та вдосконалюють алгоритми реагування без участі людини [4]. Це стає можливим завдяки використанню нейронних мереж, глибокого навчання та хмарних обчислень, які забезпечують обробку великих обсягів інформації у реальному часі.

Паралельно з цим зростає роль етичних аспектів кібербезпеки. У світі, де межа між приватною та публічною інформацією стає дедалі тоншою, важливо зберігати баланс між безпекою та правами людини. Це стосується не лише збирання даних користувачів, а й прозорості алгоритмів, що приймають рішення на основі цих даних. Забезпечення цифрових прав, таких як право на анонімність або забуття, повинно стати невід'ємною частиною політики безпеки. Насамкінець варто підкреслити, що майбутнє інформаційної безпеки – це не ізольована боротьба з кіберзлочинністю, а інтегрована модель цифрової стійкості, де всі елементи технології, законодавство, культура поведінки функціонують як єдиний злагоджений механізм.

Окрему нішу в сучасній інформаційній безпеці займає управління інцидентами та цифрове розслідування кіберподій. У випадку порушення захисту інформаційної системи важливо не лише швидко ліквідувати наслідки атаки, а й визначити її джерело, цілі, механізм проникнення та потенційні вразливості, що були використані [2]. Для цього все частіше застосовуються інструменти цифрової криміналістики, що дозволяють відновлювати послідовність подій у кіберпросторі з високою точністю.

Інша тенденція, яка набирає обертів, – це перехід до концепції «Zero Trust Architecture» (ZTA) – це сучасний підхід до кібербезпеки, що базується на принципі «Нікому не довіряй, завжди перевіряй». Він передбачає, що доступ до ресурсів надається тільки після перевірки ідентичності користувача, пристрою та контексту запиту, незалежно від того, де знаходиться користувач. ZTA не має чітких стандартів, але базується на принципах, що застосовуються для забезпечення безпеки у різних середовищах, включаючи локальні та хмарні мережі [5].

Також важливим є питання кіберстійкості – здатності організації не лише протистояти атакам, але й швидко відновлюватися після них. У цьому контексті все більшого значення набувають плани безперервності бізнесу (BCP) та плани реагування на інциденти (IRP). Їх наявність дозволяє мінімізувати простої, зберегти дані та репутацію, що у сучасному інформаційному суспільстві може мати критичне значення.

Загалом можна констатувати, що інформаційна безпека в XXI сторіччі – це багатофакторне явище, що охоплює технології, процеси, поведінкові моделі та інституційну готовність. Її ефективність залежить не лише від рівня технічного оснащення, але й від здатності мислити на кілька кроків уперед, передбачаючи загрози ще до їх реалізації.

Висновки. Сучасна інформаційна безпека стоїть на перетині технологічного прогресу та зростаючої складності загроз, які постійно змінюються. На основі проведеного аналізу можна стверджувати, що успішне протистояння кіберзагрозам більше не може ґрунтуватися виключно на традиційних підходах або ізольованих технічних рішеннях. В умовах швидкоплинних цифрових змін критично важливо поєднувати інструменти штучного інтелекту з комплексними системами виявлення та запобігання атакам. Забезпечення захисту має відбуватися не лише на рівні інфраструктури, а й на рівні свідомості користувачів, управлінських рішень та нормативного регулювання. Успішна стратегія кіберзахисту повинна враховувати взаємозв'язок між технологіями, поведінкою людей та безперервною аналітикою ризиків. Саме така синергія дозволить сформувати адаптивну систему інформаційної безпеки, здатну ефективно реагувати на загрози, які ще тільки формуються на горизонті цифрового майбутнього.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шиманський О.В. Національна система кібербезпеки України: правові та організаційні аспекти. *Інформація і право*. 2021. № 1. С. 23–31.
2. Баранов О.І. Основи інформаційної безпеки: навч. посіб. Київ : НАВС, 2021. 248 с.
3. Макєєв С.А. Інформаційна безпека держави в умовах гібридної війни. Київ: Ліра-К, 2020. 186 с.
4. Шиманський О.В. Національна система кібербезпеки України: правові та організаційні аспекти. *Інформація і право*. 2021. № 1. С. 23–31.
5. Buczak A.L., Guven E.A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18(2). P. 1153–1176.
6. Zero Trust Architecture: новий стандарт у кібербезпеці. URL: https://vamark.ua/blog/zero-trust-architecture-novyj-standart-u-kiberbezpeczi.
7. Бєлова М.В., Бєлов Д.М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід. *Аналітично-порівняльне правознавство*. № 2. 2023. С. 448–454.