КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056.5:004.492
DOI https://doi.org/10.32782/2521-6643-2026-2-72.25

Лучик С. Д., доктор економічних наук, професор,
професор кафедри інформаційних систем і технологій
Харківського національного університету внутрішніх справ
ORCID: 0000-0003-0757-1140

Заїка І. В., курсант Навчально-наукового інституту № 4
Харківського національного університету внутрішніх справ
ORCID: 0009-0006-4582-6465

Саєнко С. Л., курсант Навчально-наукового інституту № 4
Харківського національного університету внутрішніх справ
ORCID: 0009-0009-1246-2345

RANSOMWARE: МЕХАНІЗМ РОБОТИ ТА СПОСОБИ ЗАХИСТУ

Серед численних сучасних цифрових загроз шкідливі програми категорії ransomware займають унікальну позицію, створюючи небезпеку для людської безпеки та стійкості цілих секторів економіки. Потерпання організацій від ransomware, яке постійно удосконалюється, вимагає покращення рівня інформаційного захисту і надає даній тематиці соціальної значущості. Всебічне вивчення принципів функціонування ransomware, механізму дії та аналіз і оцінка ефективності методів протидії цим кіберзагрозам залишається нагальним завданням для науковців і практиків.

Метою статті є всебічний розгляд феномену ransomware – від типологічної класифікації та історичного розвитку до детального вивчення механізмів здійснення атак і розробки практичних рекомендацій щодо захисту.

У статті виділені та висвітлені історичні етапи виникнення та поширення програм-вимагачів. Досліджено алгоритм здійснення сучасної атаки ransomware з описом основних характеристик. Розглянуті ключові тенденції розвитку ransomware, які змінюють ландшафт кіберзагроз. Запропоновано ефективну систему захисту від ransomware, що поєднує технологічні, організаційні та процедурні компоненти. Виділені основні рекомендації щодо захисту інформаційних систем і технологій організацій від програм-вимагачів. Організаціям необхідно впровадити жорсткий патч-менеджмент для негайного оновлення вразливих зовнішніх сервісів, обов'язково використовувати багатофакторну автентифікацію (MFA) для всіх точок входу та регулярно проводити практичні симуляції фішингу для персоналу. Технічний захист має базуватися на обов'язковому розгортанні рішень класу EDR/XDR, які здатні автоматично блокувати аномальні дії до настання незворотних наслідків. Критично важливо впровадити наскрізне криптографічне шифрування конфіденційних даних на серверах організації (Data-at-Rest), що зробить їх марними для хакерів у разі витоку. І кожна установа повинна розробити, документально затвердити та регулярно тестувати план реагування на інциденти (Incident Response Plan), заздалегідь налагодивши канал комунікації з урядовими структурами захисту, такими як CERT-UA.

Ключові слова: *ransomware, програма-вимагач, кіберзагроза, кібератака, захист, кібербезпека, подвійне вимагання, EDR/XDR, реагування на інциденти.*

Luchyk S. D., Zaika I. V., Saienko S. L. Ransomware: mechanism of action and methods of protection

Among the many contemporary digital threats, malicious software in the ransomware category occupies a dominant and distinctive position, posing an unprecedented danger not only to data confidentiality but also to human safety and the resilience of entire sectors of the economy, including critical infrastructure and the public sector. Global digitalization, the transition to cloud technologies, and the expansion of corporate network boundaries have significantly increased the attack surface. The impact of ransomware on organizations, as it continues to evolve and become more sophisticated, results in enormous financial losses, paralysis of business processes, and reputational damage. This necessitates a fundamental reassessment of approaches to information security and gives this topic considerable social and scientific significance.

The aim of this article is to provide a comprehensive examination of the ransomware phenomenon – from typological classification and historical development to a detailed study of the technical mechanisms of attack execution and the development of comprehensive practical recommendations for protection.

The article identifies and outlines the historical stages in the emergence and spread of ransomware: from basic encryptors to modern "Ransomware-as-a-Service" (RaaS) business models, which have substantially lowered the barrier to entry for cybercriminals. The study examines the algorithm of a modern ransomware attack, with a detailed description of its key phases: initial compromise (through phishing, exploitation of RDP vulnerabilities, or zero-day vulnerabilities), lateral movement, exfiltration, and encryption.

Based on the analysis conducted, an effective ransomware protection system is proposed, grounded in the Zero Trust concept and combining technological, organizational, and procedural components. Organizations need to implement rigorous patch management to ensure the immediate updating of vulnerable services, mandatorily use multi-factor authentication (MFA) for all entry points, and regularly conduct practical phishing simulations for personnel. Technical protection should include strict network segmentation and be based on the mandatory deployment of EDR/XDR-class solutions capable of automatically blocking anomalous activities before irreversible consequences occur. It is critically important to implement end-to-end cryptographic encryption of confidential data at rest, which will render such data useless to hackers in the event of a leak, as well as to strictly adhere to the "3-2-1" backup rule with isolated copies. Every institution should develop, formally approve, and regularly test an Incident Response Plan, while establishing in advance a communication channel with governmental protection agencies such as CERT-UA.

Key words: *ransomware, cyber threat, cyber attack, protection, cybersecurity, double extortion, EDR/XDR, incident response.*

Постановка завдання. У наш час складно виявити галузь діяльності, котра не потребує стабільної роботи цифрових технологій. Критична інфраструктура, зокрема фінансовий сектор, енергетика, медицина та транспорт, нині вразлива до ризиків, що раніше мали виключно теоретичний характер. Серед численних сучасних цифрових загроз шкідливі програми категорії ransomware займають унікальну позицію – не тільки з огляду на обсяги економічних втрат, а й завдяки спроможності цілковито зупинити функціонування установ, створюючи небезпеку для людської безпеки та стійкості цілих секторів економіки.

Згідно з інформацією FinCEN (Мережі боротьби з фінансовими злочинами Сполучених Штатів), протягом трирічного періоду 2023–2025 років зареєстровані виплати потерпілих від ransomware склали понад 2,1 мільярда доларів США, водночас за дев'ятирічний період 2013–2021 років цей показник дорівнював 2,4 мільярда [1]. Отже, швидкість наростання збитків зростає. Протягом 2025 року у глобальному масштабі задокументовано 6 311 верифікованих ransomware-атак, тобто спостерігається зростання на 13 % порівняно з попереднім роком, при цьому останній квартал охопив 30 % всіх зафіксованих випадків за рік. Паралельно збільшується і тактична витонченість нападів. Якщо раніше зловмисне програмне забезпечення лише кодувало інформацію і очікувало на грошовий переказ, сьогодні переважна більшість злочинних груп викрадаєінформацію і паралельно через публічні канали чинить психологічний тиск та залякує власників розголошенням їх даних.

Потерпання організацій від ransomware, яке постійно удосконалюється, вимагає покращення рівня інформаційного захисту і надає даній тематиці соціальної значущості. Саме тому всебічне вивчення принципів функціонування ransomware, механізму дії та аналіз і оцінка ефективності методів протидії цим кіберзагрозам залишається нагальним завданням для науковців і практиків.

Аналіз останніх досліджень і публікацій. Тематика шкідливого програмного забезпечення типу вимагачів привертає увагу фахівців з багатьох держав. Серед закордонних авторів даної тематики варто виділити кілька напрямів дослідження.

Технологічний розгляд принципів ransomware та підходів до ідентифікації зловмисного коду висвітлено, зокрема, у дослідженні А. Газет [2], де проведено компаративний розбір початкових варіантів програм-вимагачів за криптографічними та поведінковими характеристиками. У масштабному систематичному дослідженні [3], автори: М. Рехман, М. Фадзіл Хассан, Р. Акбар та інші, узагальнюють методики раннього виявлення ransomware за період 2021–2025 років. Дані праці формують фундаментальне розуміння «будови» атаки, хоча, за словами самих дослідників, значний відсоток наявних підходів сфокусований на застарілих варіантах криптографічного ransomware і не враховує сучасних схем з крадіжкою даних.

Трансформацію моделей кіберзлочинності, зокрема, перехід від поодиноких атак до структурованих RaaS-платформ, детально досліджено у праці Л. Й. Конноллі та Д. С. Волла [4], яка стала одним із перших комплексних досліджень нового ландшафту цифрових загроз. Автори переконливо демонструють, що експансія криптовалют фундаментально змінила економічну модель ransomware, тобто зменшились ризики для зловмисників і паралельно ускладнилась діяльність правоохоронних органів.

Криптографічний аспект кібератак, передусім застосування гібридних схем кодування, всебічно розкрито у фундаментальній роботі В. Сталлінгса [5], котра слугує методологічною базою для усвідомлення математичної надійності сучасних програм-вимагачів. Організаційні виміри протидії та значущість людського чинника як первинної точки проникнення програми досліджено у статті Сінь (Роберт) Ло та Цінью Ляо [6], де обґрунтовано пріоритетність освіти персоналу над виключно технологічними засобами захисту від кібератак.

Комплексні дослідження Verizon Business [7], Sophos [8, 9, 10], Europol [11] містять актуальний статистичний зріз небезпек і є незамінним ресурсом для розуміння поточних трендів. Зокрема, у дослідженні

А. В. Шуайб, Аун Їчіет та інші [12] здійснено глибокий розбір еволюції ransomware з акцентуванням на феномені «подвійного шантажу», а М. Бенмалек [13] розглядає специфіку атак на кіберфізичні системи, зокрема об'єкти критичної інфраструктури.

Що стосується вітчизняної наукової думки, питання захисту інформаційної інфраструктури від кібератак знайшли відображення у публікаціях, присвячених загальним засадам кібербезпеки в Україні, а особливої актуальності набули у зв'язку з повномасштабним вторгненням 2022 року: аналіз кіберінцидентів проти українських інституцій у цей період представлено, зокрема у звітах CERT-UA [12].

Водночас у літературі залишаються недостатньо висвітленими питання комплексного підходу до захисту від програм-вимагачів, який би поєднував технічні та організаційні заходи в єдину систему з урахуванням найновіших тенденцій їх використання, зокрема, поширення тактики «потрійного вимагання» та використання штучного інтелекту зловмисниками для масштабування фішингових кампаній. Саме це визначає потребу в систематизувальному дослідженні, здатному узагальнити наявні знання та сформулювати практичні рекомендації для різних категорій організацій.

Метою статті є всебічний розгляд феномену ransomware – від типологічної класифікації та історичного розвитку до детального вивчення механізмів здійснення атак і розробки практичних рекомендацій щодо захисту. Для реалізації встановленої мети розв'язуються наступні завдання: по-перше, вивчення головних векторів початкового інфікування систем та їх статистичного розподілу у сучасних кампаніях; по-друге, розгляд послідовності стадій атаки та криптографічних методик, що використовуються зловмисниками; по-третє, характеристика актуальних тенденцій еволюції кіберзлочинних схем із врахуванням свіжих даних; по-четверте, визначення результативних організаційних і технічних заходів протидії та формування покрокового алгоритму реагування на інциденти.

Виклад основного матеріалу. Термін «ransomware» охоплює категорію шкідливого програмного забезпечення, спільною рисою якого є обмеження доступу користувача до власної інформаційної системи або даних із наступною вимогою викупу задля відновлення цього доступу. Залежно від механізму впливу ці програми поділяються на кілька основних типів.

Найпоширенішим є crypto-ransomware, який застосовує криптографічні алгоритми для блокування файлів, баз даних або цілих дискових розділів. Операційна система при цьому може залишатися частково працездатною, однак уся цінна інформація стає недоступною без ключа дешифрування. Принципово відмінним видом є locker-ransomware. Він не обов'язково шифрує вміст диска, але блокує інтерфейс користувача або унеможливлює завантаження системи, відображаючи повідомлення про необхідність оплати. Окрему нішу займають leakware (або doxware), тобто програми, орієнтовані насамперед на викрадення конфіденційних даних із погрозою їх публічного оприлюднення. Нарешті, сучасні атаки дедалі частіше поєднують усі ці підходи в межах одного інциденту, утворюючи гібридні моделі з максимальним тиском на жертву.

Щоб усвідомити масштаб сучасної небезпеки від програм-вимагачів, варто звернутися до історії їх виникнення. Перший відомий зразок програми-вимагача – це троян AIDS, який відомий як PC Cyborg. Він'явився у 1989 році і його автор, доктор Джозеф Попп, розповсюдив близько 20 000 інфікованих дискет серед учасників конференції ВООЗ з проблем СНІДу. Троян шифрував імена файлів на диску С і вимагав надіслати 189 доларів поштовим переказом на адресу в Панамі [3]. З технічної точки зору ця програма була примітивною і алгоритм шифрування легко піддавався злому. Проте сама концепція виявилася живучою.

Справжній прорив у становленні програм ransomware відбувся на початку 2010-х років, коли злочинці почали впроваджувати стійке асиметричне кодування та цифрові валюти для анонімного отримання коштів. Показовим випадком стало розповсюдження CryptoLocker у 2013 році: протягом перших кількох місяців дане шкідливе програмне забезпечення (ШПЗ) інфікувало понад 250 000 комп'ютерів і принесло своїм розробникам, за різними оцінками, від 3 до 27 мільйонів доларів [4]. Це наочно продемонструвало, що ransomware може бути надзвичайно прибутковим бізнесом.

Критичним моментом, після якого ставлення до кіберзагроз у всьому світі змінилося, стала атака вірусу-хробака WannaCry у травні 2017 року. Експлуатуючи вразливість у протоколі SMB, задокументовану під кодовою назвою EternalBlue, і створену, за наявними свідченнями, Агентством національної безпеки США, WannaCry поширювався між комп'ютерами без потреби у взаємодії з користувачем. Протягом кількох діб цей вірус інфікував понад 300 000 комп'ютерів у 150 країнах, спричинивши збитки, що оцінюються у чотири мільярди доларів США [4]. Особливо сильно постраждала британська Національна служба охорони здоров'я (NHS), де через зупинку систем довелося скасувати близько 20 000 запланованих медичних процедур. Всього через місяць аналогічний напад NotPetya, що вибірково націлювався на українські організації, завдав збитків понад 10 мільярдів доларів, ставши, за оцінками фахівців, найдорожчою кібератакою в історії.

Після цих подій індустрія кіберзлочинності перейшла на нову організаційну модель – Ransomware-as-a-Service (RaaS), котра забезпечує поділ праці між розробниками шкідливих програм та їхніми операторами. Провідні RaaS-угруповання, такі як LockBit, ALPHV (BlackCat), Cl0p та Akira, функціонують як повноцінні корпоративні структури. Вони пропонують технічну підтримку 24/7, регулярно оновлюють шкідливе ПЗ для обходу антивірусних засобів і навіть проводять маркетингові кампанії для залучення нових «афіліатів» – хакерів, які виконують самі атаки, отримуючи за це 70–80 % від викупу. Згідно з даними NCC Group

Threat Pulse, протягом 2024 року найактивнішим угрупованням виявився LockBit з 696 задокументованими атаками, друге місце посіло RansomHub (353 атаки), третє – Play (317 атак) [5].

Сучасна атака ransomware відбувається за чітко структурованою послідовністю етапів. Початковий етап – первинне проникнення (Initial Access) – здійснюється переважно через три основні вектори (рис. 1). Згідно з даними Sophos за 2025 рік, 32 % атак відбулися через невідпатчені вразливості у програмному забезпеченні, 23 % – через скомпрометовані облікові дані (часто здобуті внаслідок фішингу чи витоку баз даних), а 18 % – через успішні фішингові листи з макросами або вкладеними зловмисними файлами. Вразливості у публічно доступних додатках – зокрема Apache Log4Shell (CVE-2021-44228) та MOVEit Transfer (CVE-2023-34362) – дозволяють зловмисникам виконувати код дистанційно без автентифікації [8].

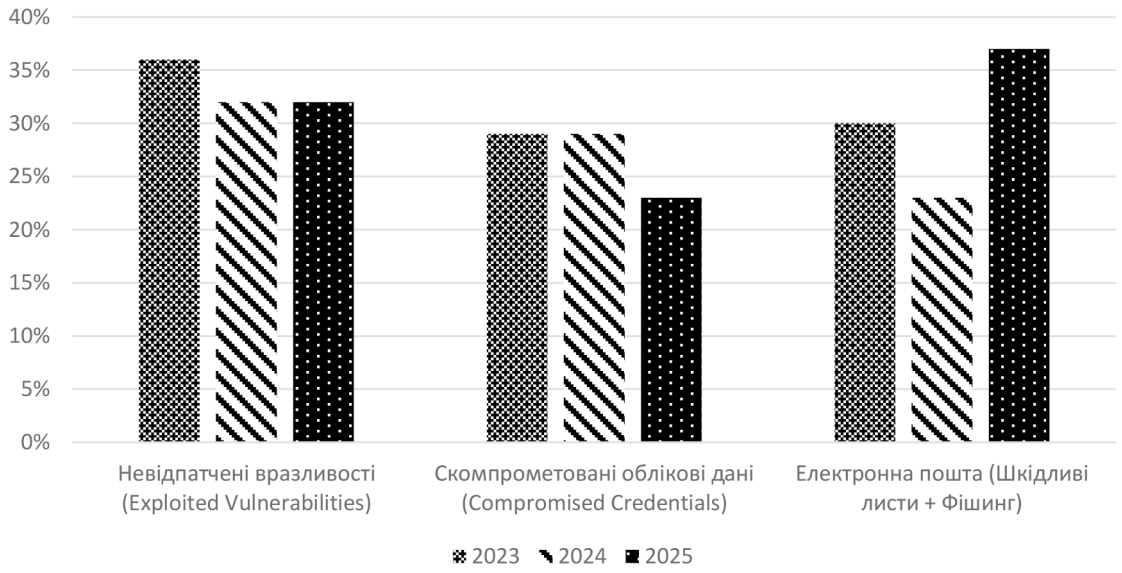

Рис. 1. Динаміка векторів первинного проникнення ransomware у 2023–2025 рр.

Джерело: [8, 9, 10].

Після успішного проникнення атакуючі переходять до етапу закріплення (Persistence and Privilege Escalation), коли створюються постійні точки входу в систему та здобуваються привілеї адміністратора. Найчастіше використовують модифікацію реєстру Windows, створення заданих завдань (Scheduled Tasks), експлуатацію системних утиліт на кшталт PsExec чи Mimikatz для викрадення токенів аутентифікації [5]. Паралельно зловмисники вимикають антивірусні рішення та засоби моніторингу безпеки, використовуючи штатні інструменти операційної системи, щоб уникнути виявлення.

Третій етап – розвідка та латеральне переміщення (Reconnaissance and Lateral Movement) – полягає у картографуванні мережі організації, виявленні критичних серверів і поширенні на інші вузли. Атакуючі сканують доменні контролери, файлові сервери, бази даних і системи резервного копіювання за допомогою інструментів Active Directory reconnaissance (BloodHound, ADFind) та використовують легітимні протоколи (RDP, SMB, WMI) для переміщення між системами. На цій стадії особливу увагу зловмисників привертають сервери резервних копій, оскільки їх знищення позбавляє організацію можливості безкоштовного відновлення даних.

Четвертий етап – ексфільтрація даних (Data Exfiltration) – став стандартом після 2019 року і використовується у більшості сучасних атак. Зловмисники копіюють конфіденційну інформацію на зовнішні сервери, застосовуючи хмарні сервіси (MEGA, Dropbox, AWS S3), FTP-передачу або спеціалізовані інструменти, такі як Rclone та FileZilla. За даними звіту Sophos 2024, у 32 % випадків атакуючі викрадали дані, навіть якщо жертва мала функціонуючі резервні копії, використовуючи погрозу публікації як додатковий важіль тиску.

Завершальний етап – шифрування та вимога викупу (Encryption and Ransom Demand) – активується у заздалегідь обраний час, здебільшого вночі або у вихідні дні, коли IT-персонал недоступний. Сучасні програми-вимагачі використовують гібридні криптографічні схеми: генерується випадковий симетричний ключ (AES-256 або ChaCha20), яким швидко кодуються файли, а сам цей ключ шифрується асиметричним алгоритмом (RSA-4096 або еліптичними кривими), що робить розшифрування без приватного ключа атакуючого математично неможливим [5]. Після шифрування на екрані з'являється повідомлення з інструкціями щодо оплати викупу (зазвичай у Bitcoin чи Monero) та посиланням на сайт у мережі Tor для переговорів. Деякі угруповання додають таймер обіцяють подвоїти суму через кілька днів або опублікувати викрадені дані.

Протягом 2024–2025 років спостерігається низка ключових тенденцій розвитку ransomware, які змінюють ландшафт загроз.

По-перше, атаки дедалі більше концентруються на критичній інфраструктурі. За даними KELA [15], близько 50 % усіх ransomware-атак у 2025 році спрямовані на п'ять пріоритетних галузей: виробництво (21 %), охорону здоров'я (11 %), енергетику (9 %), фінансові послуги (5 %) та освіту (4 %). Особливу занепокоєність викликають атаки на медичні заклади, де простій систем може безпосередньо загрожувати життю пацієнтів. У лютому 2024 року ransomware-атака на мережу Change Healthcare, яка обробляє третину всіх медичних транзакцій США, паралізувала роботу тисяч лікарень та аптек, спричинивши збитки понад 872 мільйони доларів [14].

По-друге, поширюється тактика «потрійного вимагання» (triple extortion). Тобто зловмисники, крім шифрування файлів та погроз публікації даних, здійснюють DDoS-атаки на публічні веб-сервіси організації або безпосередньо контактують із клієнтами та партнерами потерпілої компанії, інформуючи їх про витік даних та додатково тиснучи на керівництво. Деякі угруповання навіть інформують регуляторні органи про порушення GDPR чи інших норм захисту даних, щоб спровокувати додаткові штрафи для жертви. За даними Cyberint, у 2024 році зареєстровано 95 активних ransomware-груп (проти 68 у 2023 році), а середній розмір вимоги викупу зріс до 2,73 мільйонів доларів [18].

По-третє, зловмисники активно впроваджують штучний інтелект (ШІ) для масштабування своїх операцій. Так, генеративні мовні моделі використовуються для створення переконливих фішингових листів на кількох мовах, глибоке навчання (deep learning) – для автоматичної ідентифікації цінних даних у викрадених файлах, а машинне навчання – для обходу систем виявлення поведінкових аномалій. Паралельно розвиваються і засоби захисту на базі ШІ, що призводить до своєрідної технологічної гонки озброєнь.

По-четверте, спостерігається зростання використання «безфайлових» (fileless) технік. Це коли шкідливий код виконується безпосередньо в оперативній пам'яті без збереження на диску, що ускладнює його виявлення традиційними антивірусними засобами. Атакуючі все частіше використовують легітимні системні утиліти (Living-off-the-Land Binaries, LoLBins) на кшталт PowerShell, WMI, certutil для виконання своїх завдань, що робить активність важковідрізнимою від нормальних адміністративних операцій.

Динаміка розподілу ransomware-атак за ключовими галузями економіки у 2023–2025 роках представлено на рис. 2.

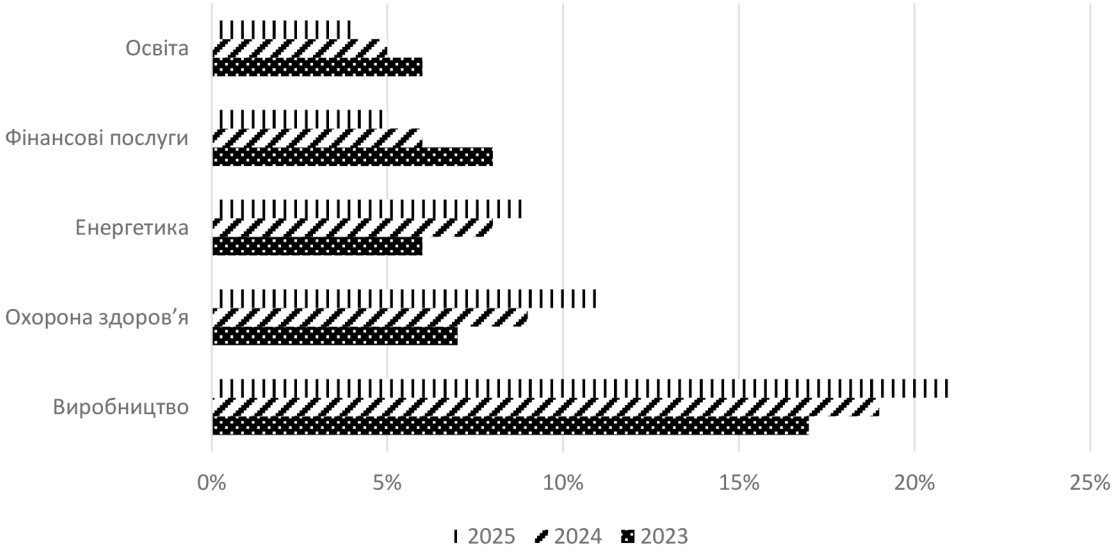

Рис. 2. Динаміка розподілу ransomware-атак за ключовими галузями економіки 2023–2025 роки

Джерело: [15, 16, 17].

Результати досліджень. Створення ефективної системи захисту від ransomware потребує комплексного підходу, що поєднує технологічні, організаційні та процедурні компоненти. На технічному рівні критично важливим є своєчасне оновлення програмного забезпечення та усунення вразливостей. Згідно з даними Verizon DBIR 2024, 94 % успішних ransomware-атак використовують публічно відомі вразливості, для яких патчі вже доступні [7]. Це означає, що організації повинні впровадити жорсткий патч-менеджмент із пріоритизацією критичних оновлень для зовнішніх сервісів протягом 24–48 годин з моменту випуску патча.

Обов'язковим елементом захисту є багатофакторна автентифікація (MFA) для всіх точок віддаленого доступу та привілейованих облікових записів. Навіть якщо злочинці здобули пароль через фішинг або витік бази даних, відсутність другого фактора (токена, біометрії, одноразового коду) суттєво ускладнює їм проникнення. За даними Microsoft, MFA блокує понад 99,9 % автоматизованих атак на облікові записи.

Розгортання рішень класу EDR (Endpoint Detection and Response) або XDR (Extended Detection and Response) дозволяє виявляти та автоматично блокувати підозрілу активність на ранніх стадіях атаки – до початку шифрування. Ці системи аналізують поведінку процесів, виявляють аномалії (несподіване відкриття великої кількості файлів, спроби видалення резервних копій, зміни в реєстрі) та можуть ізолювати заражений хост від мережі за лічені секунди. Згідно з тестами SE Labs та MITRE ATT&CK Evaluations, провідні EDR-рішення (Microsoft Defender, CrowdStrike Falcon, SentinelOne) демонструють понад 95 % ефективності виявлення тактик LockBit та інших актуальних угруповань [16].

Сегментація мережі та принцип нульової довіри (Zero Trust) дозволяють обмежити латеральне переміщення зловмисників. Критичні системи повинні бути ізольовані в окремих VLAN із суворим контролем доступу, а міжсегментний трафік фільтруватися через міжмережеві екрани нового покоління (NGFW) із функціями глибокої інспекції пакетів (DPI) та виявлення вторгнень (IDS/IPS).

Резервне копіювання даних залишається критичною лінією оборони, але повинно відповідати кільком принципам. Класичне правило «3-2-1» передбачає наявність трьох копій даних на двох різних носіях, одна з яких зберігається офлайн або в «незмінному» (immutable) сховищі, де видалення чи модифікація неможливі протягом визначеного періоду. Додатково варто тестувати процедури відновлення щонайменше раз на квартал, оскільки резервні копії, які не можна відновити, марні. За статистикою Sophos, організації з актуальними офлайн-резервними копіями відновлюються у середньому на 60 % швидше і витрачають на 40 % менше коштів порівняно з тими, хто сплачує викуп [8].

Шифрування критичних даних у стані спокою (Data-at-Rest Encryption) робить викрадену інформацію марною для зловмисників, навіть якщо їм вдалося ексфільтрувати файли. Якщо дані на серверах організації зашифровані власними ключами, хакери отримають лише нечитабельний набір байтів, що позбавляє їх можливості шантажувати публікацією. Використання рішень класу Hardware Security Module (HSM) або хмарних служб управління ключами (Key Management Service) забезпечує додатковий захист криптографічних ключів.

На організаційному рівні вкрай важливою є освіта персоналу. Оскільки 18 % атак починаються з фішингових листів, регулярні навчання співробітників розпізнаванню підозрілих повідомлень та симуляції фішингу дозволяють зменшити цей ризик. Дослідження Luo та Liao [6] показує, що організації, які проводять щоквартальні тренінги з кібербезпеки, фіксують на 70 % менше успішних фішингових атак порівняно з тими, що проводять навчання раз на рік або взагалі не проводять

Кожна установа повинна мати задокументований та регулярно тестований план реагування на інциденти (Incident Response Plan), котрий чітко визначає ролі відповідальних осіб, процедури ізоляції заражених систем, канали комунікації з урядовими CERT-командами та критерії прийняття рішень. У випадку атаки на українські організації негайний контакт із CERT-UA (cert.gov.ua) дозволяє отримати оперативну технічну підтримку та координацію з правоохоронними органами.

Якщо організація все ж таки стала жертвою ransomware-атаки, критично важливо дотримуватися чіткого алгоритму дій. По-перше, необхідно негайно ізолювати заражені системи від мережі, вимкнувши мережеві адаптери або фізично від'єднавши кабелі, щоб запобігти подальшому поширенню. По-друге, слід зберегти всі докази – логи, зразки шкідливого ПЗ, повідомлення вимагачів – для подальшого аналізу та можливого залучення правоохоронних органів. По-третє, активувати план реагування на інциденти та сповістити відповідну команду безпеки. По-четверте, провести первинну оцінку масштабу ураження: які системи заблоковані, чи були викрадені дані, чи доступні резервні копії. По-п'яте, повідомити про інцидент CERT-UA та, за необхідності, регуляторні органи (відповідно до вимог GDPR або інших норм захисту даних). По-шосте, розпочати відновлення з перевірених резервних копій паралельно з проведенням forensic-аналізу для виявлення початкового вектора атаки та всіх скомпрометованих облікових записів.

Щодо оплати викупу, то більшість експертів та урядових агенцій (включаючи FBI, CERT-UA, Europol) категорично не рекомендують платити зловмисникам. По-перше, немає жодних гарантій, що після оплати ви отримаєте робочий ключ дешифрування (за даними Sophos, у 8 % випадків платники взагалі не отримують ключ [8]). По-друге, оплата фінансує подальший розвиток кіберзлочинності та робить вашу організацію привабливою мішенню для повторних атак. По-третє, у деяких юрисдикціях оплата викупу певним угрупованням може порушувати санкційне законодавство. Якщо наявні актуальні резервні копії та система відновлення протестована, повернення до роботи без оплати є оптимальним варіантом.

Окремої уваги заслуговує ситуація в Україні, де кіберзагрози набули особливого виміру в умовах повномасштабної війни. Російські APT-угруповання (такі як Sandworm, APT28, Turla) та проксі-групи активно атакують українську критичну інфраструктуру з метою дестабілізації та підриву довіри до державних інституцій. Згідно зі звітом CERT-UA за 2024 рік, кількість зафіксованих кіберінцидентів зросла на 37,4 % порівняно з попереднім роком, досягнувши 5 927 випадків.

Тенденція до ескалації зберігається: якщо у 2024 році було опрацьовано 5 927 кіберінцидентів (на 37,4 % більше, ніж роком раніше), то у 2025 році CERT-UA продовжує фіксувати в середньому 15 інцидентів щодня, відстежуючи понад 150 угруповань (UAC). Основні удари російських хакерів та кіберзлочинців спрямовані на місцеві органи влади (понад 35 % атак), сектор безпеки й оборони та урядові організації.

Важливим кроком у 2025 році стала імплементація Закону України № 4336, завдяки якому CERT-UA трансформується у національний CSIRT із розгалуженою мережею регіональних команд. Це дозволило оперативніше виявляти та блокувати масові фішингові розсилки (кількість яких зросла вдвічі) від таких угруповань як UAC-0010, а також пришвидшити ізоляцію заражених вузлів критичної інфраструктури.

Висновки. Проведений аналіз дозволяє зробити низку узагальнень, важливих як для наукового розуміння проблеми, так і для практичного застосування. Ransomware еволюціонувало від примітивних програм із поштовою адресою для оплати до складної глобальної індустрії з поділом праці, ринком послуг і мільярдними оборотами. Кількість активних угруповань зросла за рік з 68 до 95, а загальна кількість зафіксованих атак у 2024 році досягла 5 414 – і це лише підтверджені, публічно відомі випадки, тоді як, за оцінками Blackfog, близько 85 % інцидентів взагалі не стають публічними [17].

За результатами дослідження поставлених завдань можна зробити такі висновки та надати практичні рекомендації:

По-перше, основними векторами зараження у 2025 році стали невідпатчені вразливості у програмному забезпеченні (32 % атак) та скомпрометовані облікові дані (23 %). Організаціям необхідно впровадити жорсткий патч-менеджмент для негайного оновлення вразливих зовнішніх сервісів, обов'язково використовувати багатофакторну автентифікацію (MFA) для всіх точок входу та регулярно проводити практичні симуляції фішингу для персоналу.

По-друге, сучасні атаки реалізуються через кілька прихованих фаз – від розвідки до ексфільтрації даних і шифрування. Технічний захист має базуватися на обов'язковому розгортанні рішень класу EDR/XDR, які здатні автоматично блокувати аномальні дії до настання незворотних наслідків.

По-третє, актуальні тенденції 2025 року свідчать про те, що близько 50 % атак спрямовані на критичну інфраструктуру, а зловмисники дедалі частіше шантажують жертв лише викраденням даних без їх шифрування. Поряд із класичним правилом резервного копіювання «3-2-1» з імутабельним (незмінним) офлайн-сховищем, критично важливо впровадити наскрізне криптографічне шифрування конфіденційних даних на серверах організації (Data-at-Rest), що зробить їх марними для хакерів у разі витоку.

По-четверте, ефективний захист неможливий без комплексної системи. Кожна установа повинна розробити, документально затвердити та регулярно тестувати план реагування на інциденти (Incident Response Plan), заздалегідь налагодивши канал комунікації з урядовими структурами захисту, такими як CERT-UA.

Перспективи подальших досліджень пов'язані з кількома напрямами. По-перше, активний розвиток рішень на базі штучного інтелекту відкриває можливості для автоматизованого виявлення і класифікації невідомих загроз у режимі реального часу – і водночас зловмисники вже активно використовують генеративний ШІ для масштабування фішингових кампаній, що робить дослідження цієї «гонки озброєнь» особливо актуальним. По-друге, потребують глибшого вивчення правові та регуляторні механізми протидії RaaS-угрупованням на міжнародному рівні, а також питання координації між CERT-UA та аналогічними структурами країн-партнерів. По-третє, заслуговує на окремий аналіз специфіка захисту українських підприємств в умовах воєнного стану, коли кібератаки нерідко поєднуються з кінетичними ударами по інфраструктурі та вимагають особливих підходів до забезпечення безперервності бізнесу.

Список використаних джерел

1. Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024. *Financial Crimes Enforcement Network*. December 2025. U.S. Department of the Treasury. 2025. URL: https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf (date of access: 05.03.2026).

2. Gazet A. Comparative analysis of various ransomware virii. *Journal in Computer Virology*. 2010. Vol. 6, № 1. Pp. 77–90. https://doi.org/10.1007/s11416-008-0092-2

3. Rehman, M.u. et al. Analyzing Early Indicators of Ransomware: Pre-encryption Behavior Patterns. In: Mohamad, H., Hasan, M.H., Abdulkadir, S.J., Shafiq, N. (eds) *Proceedings of the International Conference on Smart Cities*. Vol. 2. ICSC 2024. *Lecture Notes in Electrical Engineering*. 2025. Vol. 1417. Springer, Singapore. https://doi.org/10.1007/978-981-96-5848-0_46

4. Connolly L. Y., Wall D. S. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*. 2019, vol. 87. Pp. 101568. https://doi.org/10.1016/j.cose.2019.101568

5. Stallings W. Cryptography and Network Security: Principles and Practice. *7th ed. Pearson Education Limited*. 2017. 766 p. URL: http://14.139.161.31/EvenSem-1225-0426/cssp/Cryptography-and-network-security-principles-and-practice.pdf (date of access: 06.03.2026).

6. Luo X., Liao Q. Awareness education as the key to ransomware prevention. *Information Systems Security*. 2007. Vol. 16, № 4. Pp. 195–202. URL: https://www.researchgate.net/publication/220450120_Awareness_Education_as_the_Key_to_Ransomware_Prevention (date of access: 09.03.2026).

7. 2025 Data Breach Investigations Report. *Verizon Business*. URL: https://www.verizon.com/business/resources/reports/dbir/ (date of access: 11.03.2026).

8. Adam S. The State of Ransomware. *Sophos*. 2025. URL: https://www.sophos.com/en-us/blog/the-state-of-ransomware-2025 (date of access: 11.03.2026).

9. Adam S. The State of Ransomware 2023. *Sophos*. 2023. URL: https://assets.sophos.com/X24WTUEQ/at/c949g76937ntnj7ptnmspw/sophos-state-of-ransomware-2023-wp.pdf (date of access: 11.03.2026).

10. Adam S. The State of Ransomware 2024. *Sophos*. 2024. URL: https://assets.sophos.com/X24WTUEQ/at/cqv6xgmpb34wjdmb8fcpkpxp/sophos-state-of-ransomware-2024-wp.pdf (date of access: 11.03.2026).

11. Steal, deal and repeat – How cybercriminals trade and exploit your data. Internet Organised Crime Threat Assessment (IOCTA 2025). *Europol*. URL: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data (date of access: 13.03.2026).

12. Wadho, S. A., Yichiet, A., Gan, M.-L., Lee, C. K., Akbar, R., & Kumar, R. Emerging Ransomware Attacks: Improvement and Remedies – A Systematic Literature Review. In 2023 *4th International Conference on Artificial Intelligence and Data Sciences* (AiDAS). DOI: 10.1109/AiDAS60501.2023.10284647. URL: https://ieeexplore.ieee.org/document/10284647 (date of access: 13.03.2026).

13. Benmalek M. Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*. Vol. 4. Pp. 186-202. https://doi.org/10.1016/j.iotcps.2023.12.001

14. War and cyber: three years of struggle and lessons for global security analytical report. 2025. Analytical report. *State Service of Special Communications and Information Protection of Ukraine*. Kyiv – 2025. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=69131 (date access: 15.03.2026).

15. Ransomware Trends & Proactive Strategies New data on rising threats & strategies for cyber resilience. *Veeam*. URL: https://surl.li/ojzjlr (date access: 15.03.2026)

16. Ransomware Victims and Network Access Sales in Q1 2023. *KELA Cyber Threat Intelligence*. 2023. URL: https://www.kelacyber.com/wp-content/uploads/2023/04/KELA_Research_Q1-2023_ransomware-and-network-access-sales.pdf (date access: 15.03.2026).

17. Kapon, B. The state of cybercrime 2024: Key Threats & What's Coming in 2025. *KELA Cybercrime Intelligence*. 2025. URL: https://www.kelacyber.com/blog/the-state-of-cybercrime-2024-key-threats-whats-coming-in-2025/ (date access: 15.03.2026).

18. UnitedHealth Group reports first quarter 2024 results. Press Release. *UnitedHealth Group*. 2024. 16 April. URL: https://www.unitedhealthgroup.com/newsroom/2024/2024-04-16-uhg-reports-first-quarter-results.html (date access: 19.03.2026).

19. Ransomware Annual Report 2024. *Cyberint*. 2025. URL: https://cyberint.com/blog/research/ransomware-annual-report-2024/ (date access:: 20.03.2026).

20. ATT&CK Evaluations: Enterprise. *MITRE*, 2025: URL: https://evals.mitre.org/enterprise/er7/ (date access:: 23.03.2026).

21. The State of Ransomware Report. *BlackFog*. 2025. URL: https://www.blackfog.com/2025-q3-ransomware-report/ (date access:: 24.03.2026).

References:

1. Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data (2025). Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024. *Financial Crimes Enforcement Network (FinCEN)*. U.S. Department of the Treasury. Retrieved from https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf (date of access: 05.03.2026) [in English].

2. Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in Computer Virology*. Vol. 6, № 1. Pp. 77–90. https://doi.org/10.1007/s11416-008-0092-2 [in English].

3. Rehman, M.U. et al. (2025). Analyzing Early Indicators of Ransomware: Pre-encryption Behavior Patterns. In: Mohamad, H., Hasan, M. H., Abdulkadir, S. J., Shafiq, N. (eds) *Proceedings of the International Conference on Smart Cities*. Vol. 2. ICSC 2024. *Lecture Notes in Electrical Engineering*, vol 1417. Springer, Singapore. Retrieved from https://doi.org/10.1007/978-981-96-5848-0_46 [in English].

4. Connolly, L. Y. & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*. Vol. 87, 101568. Retrieved from https://doi.org/10.1016/j.cose.2019.101568 [in English].

5. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. *7th ed. Pearson Education Limited*. Retrieved from http://14.139.161.31/EvenSem-1225-0426/cssp/Cryptography-and-network-security-principles-and-practice.pdf (date of access: 06.03.2026) [in English].

6. Luo, X. & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security*. Vol. 16, no. 4. Pp. 195–202. Retrieved from https://www.researchgate.net/publication/220450120_Awareness_Education_as_the_Key_to_Ransomware_Prevention (date of access: 09.03.2026) [in English].

7. Data Breach Investigations Report (2025). *Verizon Business*. Retrieved from https://www.verizon.com/business/resources/reports/dbir/ (date access: 11.03.2026) [in English].

8. Adam, S. (2025). The State of Ransomware. *Sophos*. Retrieved from https://www.sophos.com/en-us/blog/the-state-of-ransomware-2025 (date access: 11.03.2026) [in English].

9. Adam, S. (2023). The State of Ransomware 2023 (2023). *Sophos*. Retrieved from https://www.sophos.com/en-us/blog/the-state-of-ransomware-2023 (date access: 11.03.2026) [in English].

10. Adam, S. (2024). The State of Ransomware 2024 (2024). *Sophos*. Retrieved from https://www.sophos.com/en-us/blog/the-state-of-ransomware-2024 (date access: 11.03.2026) [in English].

11. Steal, deal and repeat – How cybercriminals trade and exploit your data (2025). *Internet Organised Crime Threat Assessment (IOCTA 2025)*. *Europol*. Retrieved from https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data (date of access: 13.03.2026) [in English].

12. Wadho, S. A., Yichiet, A., Gan, M.-L., Lee, C. K., Akbar, R., & Kumar, R. (2023). Emerging Ransomware Attacks: Improvement and Remedies – A Systematic Literature Review. *4th International Conference on Artificial Intelligence and Data Sciences (AiDAS)*. DOI: 10.1109/AiDAS60501.2023.10284647. 148-153. Retrieved from https://ieeexplore.ieee.org/document/10284647 (date of access: 13.03.2026) [in English].

13. Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*. Vol. 4. Pp. 186-202. https://doi.org/10.1016/j.iotcps.2023.12.001 [in English].

14. War and cyber: three years of struggle and lessons for global security analytical report (2025). Analytical report. *State Service of Special Communications and Information Protection of Ukraine*. Kyiv – 2025. Retrieved from https://cip.gov.ua/services/cm/api/attachment/download?id=69131 (date access: 15.03.2026) [in English].

15. 2025 Ransomware Trends & Proactive Strategies New data on rising threats & strategies for cyber resilience (2025). *Veeam*. Retrieved from https://surl.li/ojzjlr (date access: 15.03.2026) [in English].

16. Ransomware Victims and Network Access Sales in Q1 2023 (2023). *KELA Cyber Threat Intelligence*. Retrieved from https://www.kelacyber.com/wp-content/uploads/2023/04/KELA_Research_Q1-2023_ransomware-and-network-access-sales.pdf (date access: 15.03.2026) [in English].

17. Kapon, B. (2025). The state of cybercrime 2024: Key Threats & What's Coming in 2025. *KELA Cybercrime Intelligence*. Retrieved from https://www.kelacyber.com/blog/the-state-of-cybercrime-2024-key-threats-whats-coming-in-2025/ (date access: 15.03.2026) [in English].

18. UnitedHealth Group reports first quarter 2024 results (2024). Press Release. *UnitedHealth Group*. 16 April. Retrieved from https://www.unitedhealthgroup.com/newsroom/2024/2024-04-16-uhg-reports-first-quarter-results.html (date access: 19.03.2026) [in English].

19. Ransomware Annual Report 2024 (2025). *Cyberint*. Retrieved from https://cyberint.com/blog/research/ransomware-annual-report-2024/ (date access: 20.03.2026) [in English].

20. ATT&CK Evaluations: Enterprise (2025). *MITRE*. Retrieved from https://evals.mitre.org/enterprise/er7/ (date access: 20.03.2026) [in English].

21. The State of Ransomware Report (2025). *BlackFog*. Retrieved from https://www.blackfog.com/2025-q3-ransomware-report/ (date access: 20.03.2026) [in English].

Дата першого надходження статті до видання: 27.03.2026
Дата прийняття статті до друку після рецензування: 20.04.2026
Дата публікації (оприлюднення) статті: 30.05.2026