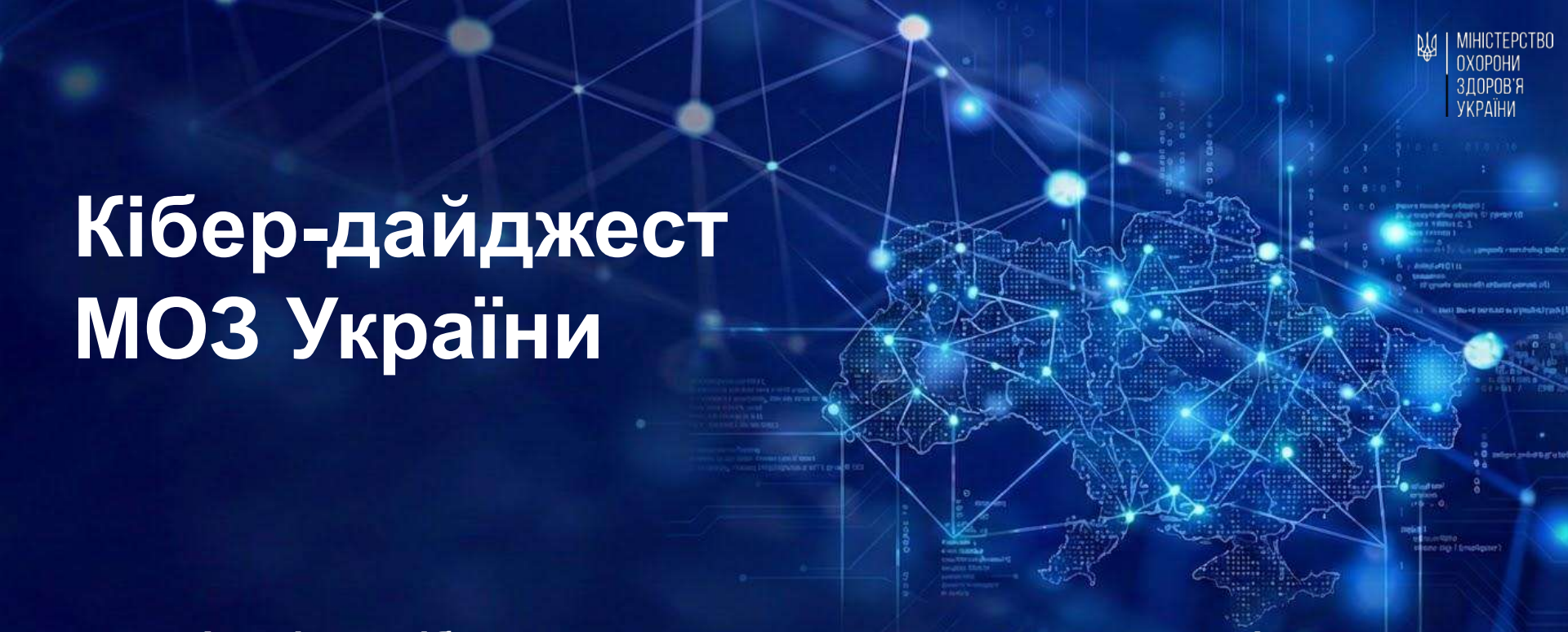
МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

# Кібер-дайджест МОЗ України



**Аналітика кіберзагроз, алгоритми захисту та актуальні вимоги державних регуляторів (ДССЗІ, НКЦК, CERT-UA)**

Травень 2026

# Державна політика кіберстійкості — Еволюція загроз та нові вимоги Держспецзв’язку до захисту ОКІ


**Суть оновлення** За даними Держспецзв’язку, фокус ворожих кібератак змістився з масованих деструктивних дій на тривале кібершпигунство та компрометацію ланцюгів постачання програмного забезпечення. Однією з таких мішеней залишаються медичні заклади та IT-підрядники. Зловмисники дедалі частіше використовують штучний інтелект для генерації фішингових розсилок (понад 1700 інцидентів у 2025 році), маскуючись під оновлення систем або повідомлення від CERT-UA. У відповідь держава посилює вимоги до стійкості: скасовано принцип «довіри за замовчуванням» для IT-постачальників, які тепер зобов'язані проходити аудит безпеки, а також розширюється застосування хмарних моделей резервного копіювання (BaaS) та аварійного відновлення (DRaaS).

**Простими словами (Оцінка ризику)** Стратегія ворога змінилася: замість спроб миттєво знищити інфраструктуру, зловмисники намагаються непомітно закріпитися в інформаційно-комунікаційних системах (ІКС) через найслабші ланки. Найчастіше такою ланкою стає персонал, який піддається маніпуляціям (через соціальну інженерію), або зовнішні компанії, що обслуговують системи закладу (атаки через ланцюг постачання). Якщо IT-підрядник скомпрометований, хакери отримують легітимний доступ до мережі закладу охорони здоров'я. Для установи це означає критичний ризик неконтрольованого витоку чутливих даних або раптової зупинки надання життєво важливих послуг через блокування ІКС. Кіберзахист сьогодні — це не просто IT-питання, а фундамент безперервності діяльності (business continuity).

**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації доцільно провести ревізію договорів та прав доступу всіх IT-підрядників. Варто переконатися, що зовнішні постачальники послуг дотримуються вимог щодо аудиту безпеки та оперативного інформування про вразливості. Також рекомендуємо провести позаплановий цільовий інструктаж персоналу щодо фішингу, акцентуючи увагу на підроблених листах, які імітують вказівки від державних органів.
2. **Відповідність нормативним вимогам**
   - Відмова від «довіри за замовчуванням» та перевірка IT-постачальників прямо відповідають вимогам Наказу ДССЗІ № 75 щодо управління ризиками ланцюга постачання (GV.SC). Формування надійних планів відновлення (зокрема за моделями BaaS/DRaaS) є обов'язковим базовим заходом (RC.RP) та невіддільною частиною підтримки цільового профілю безпеки в рамках системи управління ризиками (RMF) згідно з Постановою КМУ № 712.
3. **Стратегічне планування / Додаткова порада**
   - IT-підрозділам рекомендується розробити та формалізувати Стандартні операційні процедури (СОП) щодо безперервності діяльності та ізоляції мережі в умовах кризових ситуацій. Стратегічний фокус має бути спрямований на створення ізольованих (офлайн) резервних копій для унеможливлення тривалого простою, а також на впровадження шифрування баз даних для захисту від шантажу у разі витоку (Ransomware). Керівникам об'єктів критичної інфраструктури (ОКІ) доцільно забезпечити організаційну підтримку цих процесів на рівні управління закладом.

**Додаткові матеріали**

- ZN.UA: Полігон цифрової оборони. Як Україна будує одну з найстійкіших систем кібероборони в Європі

# Таргетований фішинг — Угруповання Ghostwriter та Gamaredon атакують державні установи України через шкідливі PDF та архіви


**Суть оновлення** Експерти зафіксували нові цілеспрямовані атаки угруповання Ghostwriter (UNC1151) та російського Gamaredon проти державних установ України. Зловмисники маскують шкідливі PDF-документи під офіційні листи від телекомунікаційних компаній (зокрема «Укртелеком»). Унікальною особливістю кампанії є використання геофенсингу: шкідливий код (PicassoLoader, що згодом завантажує бекдор Cobalt Strike) перевіряє IP-адресу і активується виключно на комп'ютерах в Україні. Паралельно Gamaredon використовує скомпрометовані державні акаунти для розсилки RAR-архівів із вірусами GammaDrop.

**Простими словами (Оцінка ризику)** Зловмисники дедалі частіше імітують листи від відомих українських контрагентів, щоб приспати пильність працівників. Перевірка IP-адреси дозволяє вірусу ховатися від міжнародних систем безпеки та активуватися лише у цільових жертв. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) це означає високий ризик того, що звичайний клік на підроблений «рахунок за зв'язок» надасть ворогу повний віддалений контроль над комп'ютером. Наслідком може стати несанкціонований доступ до інформаційно-комунікаційних систем (ІКС) та тривала зупинка операційної діяльності установи.

**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації доцільно посилити фільтрацію вхідної пошти. Рекомендуємо налаштувати додаткову перевірку підозрілих PDF-файлів із вбудованими посиланнями та RAR-архівів від невідомих відправників на рівні поштових шлюзів — це дозволить зупинити загрозу ще до того, як лист потрапить до працівника.
2. **Відповідність нормативним вимогам**
   - Забезпечення захисту від шкідливого ПЗ (PR.PT-02) та проведення інструктажів з кібергігієни (PR.AT-01) є обов'язковими базовими заходами згідно з Наказом ДССЗІ № 75. Реалізація цих кроків формує цільовий профіль безпеки в межах системи управління ризиками (RMF) та є необхідною умовою для Авторизації систем відповідно до Постанови КМУ № 712.
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується розглянути впровадження рішень класу EDR (Endpoint Detection and Response) для оперативного виявлення аномалій у пам'яті (наприклад, запуск Cobalt Strike). Керівникам установ доцільно забезпечити організаційну підтримку для розробки та дотримання Стандартних операційних процедур (СОП) щодо алгоритму дій персоналу у разі отримання підозрілих повідомлень.

**Додаткові матеріали**

- The Hacker News: Ghostwriter Targets Ukrainian Government With Geofenced PDF Phishing, Cobalt Strike — https://thehackernews.com/2026/05/ghostwriter-targets-ukrainian.html

# Вразливості інфраструктури — Критична загроза для локальних серверів Microsoft Exchange (CVE-2026-42897)


**Суть оновлення** Компанія Microsoft попередила про виявлення нової критичної вразливості (CVE-2026-42897, оцінка CVSS: 8.1) у локальних (On-Premises) версіях Exchange Server 2016, 2019 та Subscription Edition (SE). Хмарна версія Exchange Online цій загрозі не піддається. Вразливість вже активно експлуатується зловмисниками. Загроза полягає в недоліках міжсайтового скриптингу (XSS): хакерам достатньо надіслати спеціально створений електронний лист, який під час відкриття користувачем через вебінтерфейс (Outlook Web Access) дозволяє виконати довільний шкідливий JavaScript-код у браузері. Microsoft випустила офіційні патчі 9 червня 2026 року та закликає застосувати їх разом із механізмами екстреного пом'якшення.

**Простими словами (Оцінка ризику)** Якщо заклад охорони здоров'я чи об'єкт критичної інфраструктури (ОКІ) розміщує корпоративну пошту на власних фізичних серверах, він знаходиться під прямою загрозою. Для успішного зламу працівнику навіть не потрібно завантажувати вкладення чи переходити за посиланнями — достатньо просто відкрити лист у браузері. Це дозволяє зловмисникам перехопити активну сесію користувача, отримати негласний доступ до службового листування та потенційно використати скомпрометований акаунт для подальшого проникнення глибоко у внутрішню мережу установи. Наслідком може стати втрата контролю над інформаційно-комунікаційними системами (ІКС), компрометація даних та тривале порушення безперервності операційних процесів.

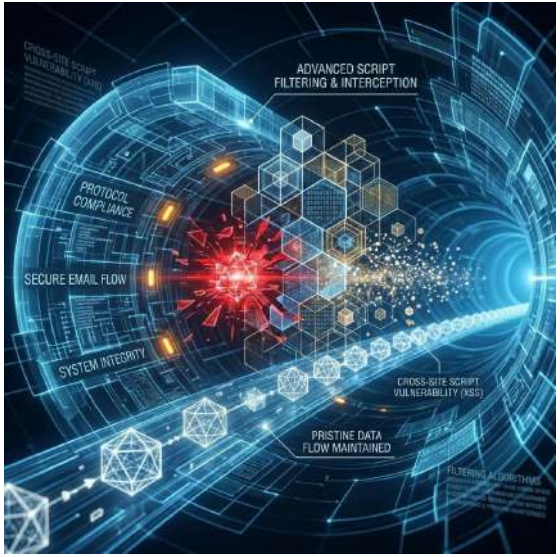
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - ІТ-підрозділам доцільно перевірити статус роботи служби екстреного пом'якшення (Exchange Emergency Mitigation Service) або вручну запустити скрипт EOMT для тимчасового блокування загрози. Також рекомендується у найкоротші терміни запланувати та встановити офіційні оновлення безпеки від Microsoft (від 9 червня 2026 року), зберігши при цьому активними превентивні механізми захисту.
2. **Відповідність нормативним вимогам**
   - Своєчасне усунення критичних вразливостей в ІКС (Patch Management) є обов'язковим базовим заходом кіберзахисту згідно з Наказом ДССЗІ № 75, зокрема пунктів ID.RA-01 (Оцінка вразливостей активів) та PR.PS-02 (Належне обслуговування ПЗ). Виконання цих вимог є невіддільною частиною підтримання цільового профілю безпеки в межах переходу на систему управління ризиками (RMF) відповідно до Постанови КМУ № 712.
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується розробити Стандартні операційні процедури (СОП) щодо екстреного патчингу критичних інфраструктурних сервісів у неробочий час для забезпечення безперервності послуг. Керівникам варто підтримати проведення цих робіт та, спираючись на аналіз ризиків, розглянути стратегічну доцільність поступової міграції на захищені хмарні поштові сервіси, які мають автоматизований цикл оновлень та не вразливі до цього класу атак.

**Додаткові матеріали**

- The Hacker News: On-Prem Microsoft Exchange Server CVE-2026-42897 Exploited via Crafted Email — https://thehackernews.com/2026/05/on-prem-microsoft-exchange-server-cve.html

# Операційне реагування — Використання інтерактивних пісочниць для превентивного захисту від складного фішингу




**Суть оновлення** Сучасні фішингові кампанії суттєво еволюціонували: вони успішно обходять статичні поштові фільтри, використовують динамічні CAPTCHA-перевірки та здатні перехоплювати OTP-коди багатофакторної автентифікації (MFA). Аналітики наголошують на критичній важливості переходу від ізольованого аналізу підозрілих посилань до використання інтерактивних хмарних пісочниць (на прикладі ANY.RUN) та інтегрованих платформ кіберрозвідки (Threat Intelligence). Це дозволяє безпековим командам за лічені секунди (до 40 секунд) повністю розкрити весь ланцюг атаки, виявити приховані поведінкові індикатори компрометації (IoC) та передати їх у корпоративні системи захисту (SIEM/SOAR/Firewalls) для блокування пов'язаної інфраструктури ворога.

**Простими словами (Оцінка ризику)** Один необережний клік працівника на фішингове посилання, замасковане під звичайне робоче запрошення, може миттєво скомпрометувати його службовий обліковий запис. Традиційні засоби захисту часто пропускають такі загрози, якщо хакери ховають шкідливий код за легітимними хмарними сервісами або використовують інструменти віддаленого адміністрування (RMM). Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) це створює ризик тривалого та непомітного перебування ворога в мережі. Хакери отримують доступ до внутрішніх інформаційно-комунікаційних систем (ІКС), що загрожує несанкціонованим витоком даних та зупинкою надання послуг. Швидкість аналізу загрози (MTTR) безпосередньо визначає, чи залишиться інцидент локальним збоєм на одному комп'ютері, чи переросте в масштабне блокування інфраструктури та порушення безперервності діяльності (business continuity).

**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації та кіберзахисту доцільно інтегрувати використання спеціалізованих інтерактивних середовищ (хмарних пісочниць) у щоденні операційні процеси обробки інцидентів. Це дозволить безпечно аналізувати вкладення та посилання в ізольованому контурі, оперативно виявляти приховані IoC (наприклад, специфічні запити до директорій чи завантаження стороннього ПЗ) та автоматично оновлювати правила фільтрації на корпоративних міжмережевих екранах.
2. **Відповідність нормативним вимогам**
   - Впровадження швидкого тріажу інцидентів та використання інструментів Threat Intelligence відповідає вимогам Наказу ДССЗІ № 75, зокрема функціям «Виявлення» (DE.CM-01: Мережевий моніторинг) та «Реагування» (RS.AN-01: Аналіз виявлених інцидентів). Автоматизація збору індикаторів компрометації посилює локальну систему управління ризиками (RMF) та допомагає підтримувати актуальний цільовий профіль безпеки для забезпечення безперервної Авторизації систем за Постановою КМУ № 712.
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується актуалізувати внутрішні регламенти (СОПи) щодо обробки інцидентів, змістивши фокус оцінки ефективності на метрики швидкості виявлення, локалізації та відновлення (MTTR). Керівникам установ варто забезпечити організаційну та фінансову підтримку модернізації інструментарію операційного центру безпеки (SOC), що дозволить суттєво знизити навантаження на першу лінію технічної підтримки та зменшити втому від надмірної кількості сповіщень (alert fatigue).

**Додаткові матеріали**

- The Hacker News: How to Reduce Phishing Exposure Before It Turns into Business Disruption — https://thehackernews.com/2026/05/how-to-reduce-phishing-exposure-before.html

# Вектори атак — Ідентифікаційні дані (Identity) стають головним шляхом компрометації систем


**Суть оновлення** За даними аналітиків IBM та Palo Alto, понад 30% усіх успішних кібератак (і понад 90% розслідуваних інцидентів) починаються з використання викрадених або неправильно налаштованих облікових даних (Identity). Зловмисникам більше не потрібно писати складні віруси — їм достатньо "просто увійти". Головна проблема полягає в тому, що класичні засоби захисту (IGA, PAM) контролюють ідентифікацію як "периметр" (на вході), але не бачать, як дрібні дозволи формують небезпечні ланцюги. Наприклад, кешований ключ на одному комп'ютері може дати доступ до Active Directory, звідти — до хмарного середовища, а потім — до баз даних. Окрему загрозу становлять "машинні" ідентифікатори (API-ключі, сервісні акаунти та ШІ-агенти), викрадення яких стрімко зростає.

**Простими словами (Оцінка ризику)** Уявіть, що ви поставили броньовані двері на вході в клініку (сильний пароль), але всередині залишили відчиненими всі кабінети, серверну та сейф із ліками. Якщо зловмисник знайде хоча б один старий "ключ" (наприклад, забутий тестовий акаунт звільненого підрядника), він зможе безперешкодно рухатися всією установою. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) надмірні права доступу — це прихована бомба. Вона дозволяє хакерам непомітно дістатися до критичних інформаційно-комунікаційних систем (ІКС), що загрожує повним паралічем роботи закладу або витоком даних.

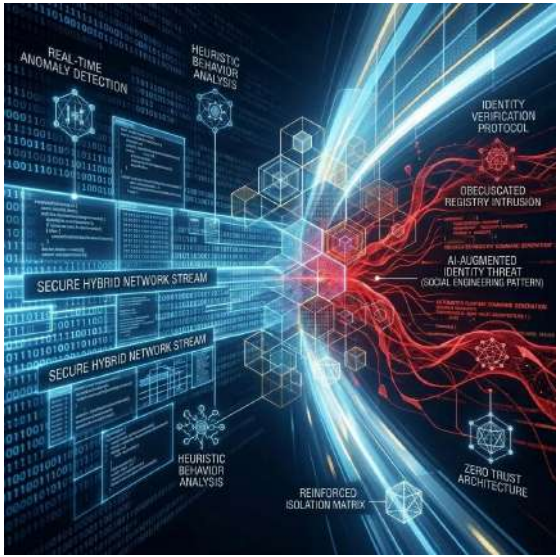
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації доцільно провести терміновий аудит облікових записів. Особливу увагу слід звернути на виявлення та видалення "мертвих" акаунтів, кешованих облікових даних на локальних машинах та надмірних привілеїв у групах Active Directory. Також необхідно перевірити права доступу "нелюдських" ідентифікаторів (сервісних служб, засобів автоматизації).
2. **Відповідність нормативним вимогам**
   - Регулярний перегляд прав доступу та впровадження принципу "найменших привілеїв" (Least Privilege) є ключовими вимогами Наказу ДССЗІ № 75 (функція "Ідентифікація", категорія "Контроль доступу" — PR.AC). Ефективне управління ідентифікаторами унеможливлює горизонтальне переміщення хакерів у мережі та є базовим критерієм для підтримки цільового профілю безпеки в рамках системи управління ризиками (RMF).
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується розробити та впровадити Стандартні операційні процедури (СОП) щодо автоматизованого відкликання прав доступу при зміні посади або звільненні співробітника. Керівникам доцільно ініціювати розгляд впровадження систем безперервного моніторингу шляхів атак (Attack Surface Management), які здатні аналізувати інфраструктуру в комплексі, виявляючи, як саме дрібні вразливості можуть призвести до компрометації всієї мережі.

**Додаткові матеріали**

- The Hacker News: When Identity is the Attack Path — https://thehackernews.com/2026/05/when-identity-is-attack-path.html

# Таргетований фішинг — Угруповання Ghostwriter атакує держсектор через підроблені листи освітньої платформи «Prometheus»




**Суть оновлення** У травні 2026 року зафіксовано нову фішингову кампанію білоруського угруповання Ghostwriter (UAC-0057), спрямовану на державні установи України. Хакери використовують скомпрометовані облікові записи для розсилки листів, замаскованих під легітимні сповіщення онлайн-платформи «Prometheus». Атака реалізується через PDF-вкладення з посиланням на ZIP-архів. Запуск шкідливого JavaScript-файлу (`OYSTERFRESH`) непомітно прописує зашифрований код у системний реєстр Windows, що зрештою розгортає фреймворк Cobalt Strike для отримання віддаленого контролю над пристроєм. Паралельно РНБО повідомляє про активне використання спецслужбами рф інструментів штучного інтелекту (ШІ) для OSINT-розвідки, автоматизованого пошуку вразливостей та динамічного формування шкідливих команд під час виконання (at runtime).

**Простими словами (Оцінка ризику)** Зловмисники часто використовують тематику професійного розвитку та освітніх заходів як привід для проведення кампаній із соціальної інженерії. Використання ШІ дозволяє хакерам створювати фішингові листи без мовних чи логічних помилок, що значно ускладнює їх візуальне виявлення користувачами. Якщо працівник закладу охорони здоров'я або об'єкта критичної інфраструктури (ОКІ) піддасться маніпуляції та відкриє файл, зловмисники отримають тривалу, приховану присутність в інфраструктурі. Головний ризик — несанкціонований доступ до конфіденційної інформації та внутрішніх інформаційно-комунікаційних систем (ІКС). За допомогою Cobalt Strike хакери можуть повністю паралізувати операційні процеси, заблокувати доступ до життєво важливих сервісів та створити пряму загрозу безперервності діяльності (business continuity) всієї установи.

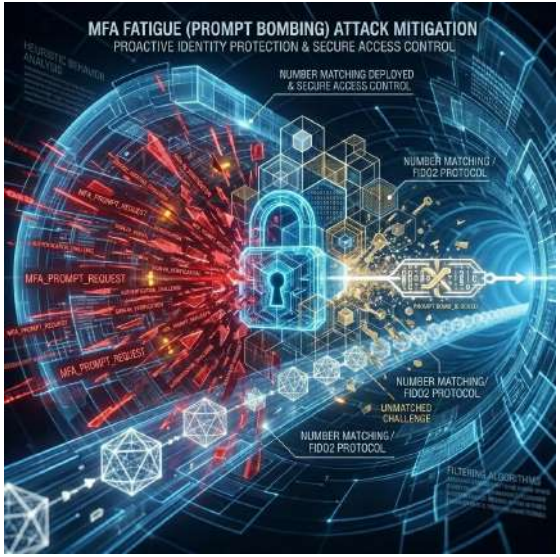
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації та кіберзахисту доцільно за допомогою групових політик (GPO) жорстко обмежити або повністю заборонити запуск штатних інструментів виконання скриптів (зокрема утиліти `wscript.exe` та `cscript.exe`) для стандартних облікових записів користувачів. Також рекомендуємо налаштувати поштові шлюзи на автоматичний карантин вхідних архівів (ZIP/RAR), які містять виконувані сценарії чи ярлики.
2. **Відповідність нормативним вимогам**
   - Технічне обмеження виконання несанкціонованого коду та оптимізація конфігурацій кінцевих пристроїв прямо відповідають вимогам Наказу ДССЗІ № 75, зокрема пунктам PR.PT-01 (Управління конфігураціями пристроїв) та PR.PS-05 (Заборона виконання несанкціонованого ПЗ). Створення таких технічних бар'єрів є обов'язковим для підтримання цільового профілю безпеки в рамках ризик-орієнтованого підходу (RMF) та успішної Авторизації систем відповідно до Постанови КМУ № 712.
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується актуалізувати Стандартні операційні процедури (СОП) щодо реагування на компрометацію облікових записів. Керівникам установ варто забезпечити планове фінансування та проведення регулярних тренінгів із кібергігієни (PR.AT-01) для персоналу, а також доручити технічним спеціалістам провести ревізію та закриття неконтрольованих або застарілих RDP- та VPN-доступів, які, за даними РНБО, залишаються основними векторами первинного проникнення.

**Додаткові матеріали**

- The Hacker News: Ghostwriter Targets Ukraine Government Entities with Prometheus Phishing Malware — https://thehackernews.com/2026/05/ghostwriter-targets-ukraine-government.html

# Соціальна інженерія — Втома від MFA (Prompt Bombing) або як хакери обходять двофакторну автентифікацію




**Суть оновлення** Багатофакторна автентифікація (MFA) більше не гарантує абсолютного захисту, якщо використовується базовий метод — push-повідомлення ("Дозволити/Відхилити" на смартфоні). Зловмисники, які вже викрали пароль користувача (з тіньових форумів чи баз даних), застосовують техніку MFA Prompt Bombing (або MFA Fatigue). Вони надсилають безперервний потік запитів на авторизацію на телефон жертви, часто підкріплюючи це телефонним дзвінком нібито від служби IT-підтримки з проханням "натиснути Дозволити, щоб зняти збій". Щойно працівник здається і натискає кнопку, хакер отримує легітимний доступ до системи та можливість зареєструвати вже власний пристрій для подальшого доступу (persistence).

**Простими словами (Оцінка ризику)** Уявіть ситуацію: працівнику о другій ночі на телефон приходить 50 сповіщень підряд із проханням підтвердити вхід до робочої пошти. А вранці "айтішник" по телефону каже: "Це був збій сервера, просто натисніть 'Так', щоб ми закрили заявку". Людина, не маючи злого умислу, підтверджує вхід, після чого ворог опиняється всередині корпоративної мережі. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) це означає неконтрольований доступ до внутрішніх систем (VPN, електронні черги, бази даних). Успішний вхід за цією схемою не викликає тривоги у систем безпеки, оскільки виглядає як звичайний логін користувача, що загрожує тривалим шпигунством або миттєвим саботажем (Ransomware) операційної діяльності установи.

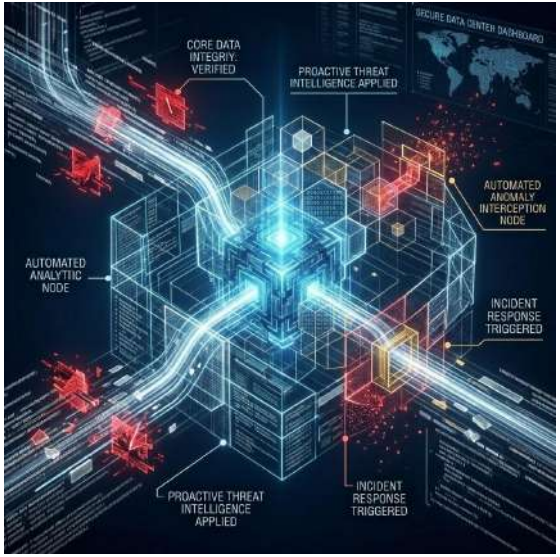
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації доцільно відмовитися від використання простих push-сповіщень ("Так/Ні") для систем MFA. Необхідно перевести всі корпоративні сервіси (зокрема VPN та пошту) на використання методів, стійких до фішингу: узгодження чисел (Number Matching в Microsoft/Google Authenticator) або використання апаратних ключів (FIDO2, YubiKey).
2. **Відповідність нормативним вимогам**
   - Впровадження надійних методів автентифікації є прямою вимогою Наказу ДССЗІ № 75 (функція "Ідентифікація", категорія "Контроль доступу" — PR.AC-07: Використання стійкої багатофакторної автентифікації). Систематичний аудит парольних політик (зокрема перевірка на використання скомпрометованих паролів з витоків) є важливою складовою підтримки цільового профілю безпеки в рамках системи управління ризиками (RMF).
3. **Стратегічне планування**
   - IT-підрозділам рекомендується розробити Стандартні операційні процедури (СОП) щодо застосування політик умовного доступу (Conditional Access). Керівникам доцільно підтримати впровадження систем, які аналізують контекст входу: якщо запит надходить із нетипової локації (наприклад, з-за кордону), з невідомого пристрою або в неробочий час, система має автоматично блокувати спробу без надсилання повідомлення на телефон користувача.

**Додаткові матеріали**

- The Hacker News: MFA Prompt Bombing: Why Your Second Factor Isn't Saving You — https://thehackernews.com/2026/05/mfa-prompt-bombing-why-your-second.html

# Операційне реагування — Сучасна парадигма SOC: запобігання інцидентам через безперервну розвідку та швидкий тріаж




**Суть оновлення** Сучасний підхід до побудови центрів управління безпекою (SOC) відходить від концепції статичного захисту периметра на користь мінімізації часу між виявленням аномалії та розумінням її суті. Експерти визначають три ключові кроки для раннього придушення загроз: безперервне оновлення систем моніторингу свіжими індикаторами компрометації (IoC) через інтеграцію з платформами Threat Intelligence (TI); миттєве збагачення (enrichment) алертів контекстом для пришвидшення ухвалення рішень (тріажу) аналітиками; та використання інтерактивних пісочниць (зокрема ANY.RUN) для безпечного запуску й аналізу підозрілих файлів і автоматичної генерації звітів для технічних та управлінських команд. Зазначається, що такий підхід суттєво знижує ймовірність розвитку прихованої активності в інцидент.

**Простими словами (Оцінка ризику)** Традиційні антивіруси та системи виявлення (SIEM) працюють ефективно лише тоді, коли їхні бази оновлюються в режимі реального часу. Якщо фахівці з безпеки закладу охорони здоров'я отримують щодня сотні розрізнених сповіщень (алертів) без контексту, вони втрачають час на ручний аналіз. Ця затримка створює "операційний борг", який зловмисники використовують для закріплення в мережі. Запізніле реагування на приховану присутність ворога в інформаційно-комунікаційних системах (ІКС) неминуче призводить до масштабних збоїв, розгортання вірусів-вимагачів (Ransomware), порушення комплаєнсу та тривалої зупинки надання послуг. Швидкість збагачення даних та автоматизованого формування звітів — це запорука збереження безперервності діяльності (business continuity).

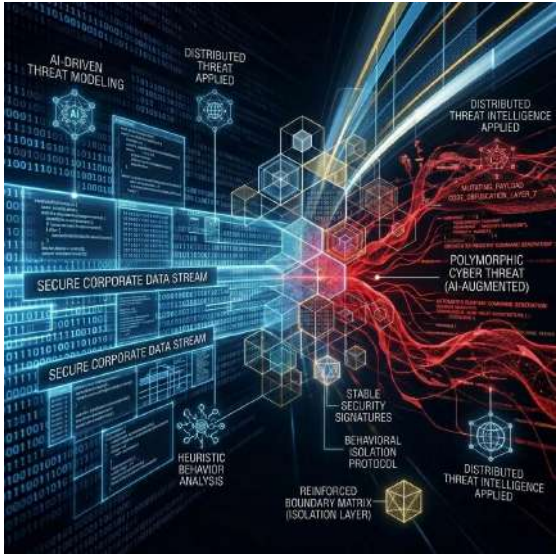
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації доцільно налаштувати автоматичну інтеграцію свіжих стрічок індикаторів компрометації (TI Feeds, наприклад, у форматах STIX/TAXII) з наявними корпоративними міжмережевими екранами та системами SIEM/EDR. Також варто оцінити можливість розгортання інструментів автоматизованого розширення алертів (TI Lookup) для зменшення кількості хибних спрацьовувань (False Positives) та навантаження на першу лінію підтримки (Tier 1).
2. **Відповідність нормативним вимогам**
   - Забезпечення системного моніторингу подій кібербезпеки та своєчасний аналіз аномалій безпосередньо відповідають вимогам Наказу ДССЗІ № 75 (функція «Виявлення», категорії DE.CM-01 та DE.AE-02). Крім того, автоматизація збору даних та інтеграція розвідувальної інформації посилюють ефективність системи управління ризиками (RMF) та сприяють підтриманню цільового профілю безпеки, необхідного для Авторизації систем згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується розробити Стандартні операційні процедури (СОП) щодо алгоритмів швидкого ухвалення рішень під час пікових навантажень на SOC. Керівникам установ доцільно сприяти впровадженню інтерактивних пісочниць та засобів автоматичної генерації звітів (зокрема з використанням ШІ-асистентів), що дозволить значно прискорити комунікацію між технічними фахівцями, менеджментом та аудиторами під час потенційних інцидентів.

**Додаткові матеріали**

- The Hacker News: 3 SOC Steps that Shut Down Incident Risks Early — https://thehackernews.com/2026/05/3-soc-steps-that-shut-down-incident.html

# Вектори атак — Нове угруповання GREYVIBE використовує штучний інтелект для кібершпигунства проти України




**Суть оновлення** Дослідники WithSecure виявили раніше недокументоване російськомовне угруповання GREYVIBE, яке з серпня 2025 року здійснює цілеспрямовані атаки проти державного, військового та цивільного секторів України. Група тісно пов'язана з кіберзлочинним екосередовищем рф та діє в інтересах кремля для збору розвідувальних даних. Зловмисники використовують широкий спектр векторів первинного проникнення: фішингові розсилки через Google Drive та хмару 4sync, підроблені сторінки перевірки CAPTCHA (маски під Zoom) та фіктивні сайти благодійних фондів допомоги ЗСУ. Головна особливість GREYVIBE — активне використання генеративного ШІ (ChatGPT, Gemini) для розробки, безперервної модифікації та обфускації шкідливого ПЗ (троянів `LegionRelay` та `PhantomRelay`), що дозволяє їм швидко змінювати технічні характеристики вірусів та обходити традиційні засоби виявлення. Шкідливе ПЗ призначене для викрадення даних браузерів, сесій месенджерів (Telegram, WhatsApp), зняття скриншотів та налаштування прихованого RDP-доступу.

**Простими словами (Оцінка ризику)** Використання супротивником комерційних платформ ШІ радикально прискорює життєвий цикл розробки шкідливого ПЗ. Хакерам більше не потрібно витрачати тижні на ручне написання унікального коду — штучний інтелект дозволяє їм миттєво рефакторити й маскувати віруси, роблячи їх невидимими для класичних антивірусів, які шукають знайомі сигнатури. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) це означає появу високодинамічної загрози. Компрометація облікових записів працівників через підроблені сторінки сервісів або фішингові вкладення відкриває зловмисникам прямий шлях до внутрішніх інформаційно-комунікаційних систем (ІКС). Головний ризик — тривале негласне перебування ворога в мережі, приховане перехоплення службових комунікацій та персональних даних, що створює передумови для масштабного витоку інформації та може призвести до раптової зупинки операційних процесів і серйозного порушення безперервності діяльності (business continuity) установи.

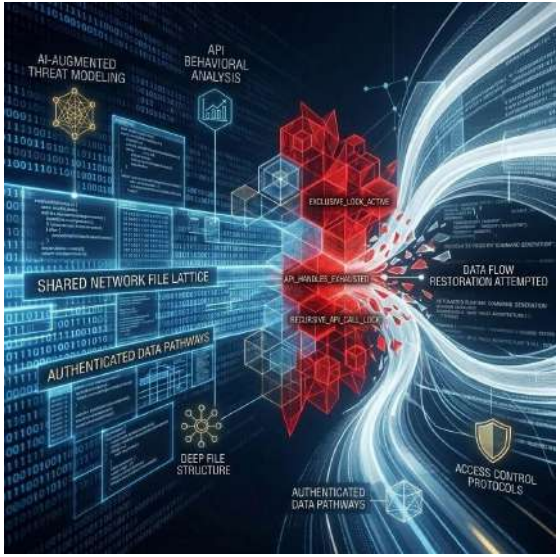
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації та кіберзахисту доцільно за допомогою групових політик (GPO) обмежити можливість виконання несанкціонованих PowerShell-скриптів та запуск командного рядка для стандартних облікових записів користувачів. Також варто налаштувати корпоративні міжмережеві екрани на блокування запитів до підозрілих публічних хмарних сховищ (як-от 4sync) та провести ревізію активних RDP-з'єднань всередині периметра інфраструктури.
2. **Відповідність нормативним вимогам**
   - Технічний контроль за використанням легітимних системних утиліт операційної системи та обмеження виконання несанкціонованого коду безпосередньо відповідають вимогам Наказу ДССЗІ № 75, зокрема заходам PR.PT-01 (Управління конфігураціями кінцевих пристроїв) та PR.PS-05 (Заборона виконання несанкціонованого програмного забезпечення). Впровадження цих обмежень є обов'язковим базовим етапом для підтримання цільового профілю безпеки ІКС та успішної Авторизації систем відповідно до Постанови КМУ № 712 в рамках ризик-орієнтованого підходу (RMF).
3. **Стратегічне планування**
   - Оскільки традиційний сигнатурний захист втрачає ефективність проти ШІ-модифікованого шкідливого ПЗ, ІТ-підрозділам рекомендується розглянути стратегічний перехід на системи поведінкового аналізу класу EDR (Endpoint Detection and Response), які аналізують аномальні дії процесів у реальному часі. Керівникам установ варто забезпечити організаційну підтримку для впровадження оновлених Стандартних операційних процедур (СОП) щодо реагування на компрометацію облікових записів та доручити технічним спеціалістам інтегрувати регулярні тренінги з кіберігієни (PR.AT-01) для персоналу з фокусом на нові техніки соціальної інженерії (фейкові вікна оновлень та CAPTCHA-перевірки).

**Додаткові матеріали**

- The Hacker News: New Russia-Linked GREYVIBE Targets Ukraine with AI-Powered Cyberattacks — https://thehackernews.com/2026/05/new-russian-linked-greyvibe-targets.html

# Загрози доступності — Інструмент GhostLock блокує доступ до файлів через легітимні функції Windows




**Суть оновлення** Дослідники безпеки попередили про появу інструменту GhostLock, який демонструє нову техніку блокування доступу до файлів на локальних дисках та мережевих ресурсах (SMB). Атака використовує легітимну функцію Windows API (`CreateFileW`), запитуючи ексклюзивний доступ до файлів (параметр `dwShareMode = 0`). У результаті операційна система відмовляє іншим користувачам та додаткам у доступі, видаючи помилку `STATUS_SHARING_VIOLATION`. Інструмент не потребує прав адміністратора і може бути запущений від імені звичайного користувача. На відміну від вірусів-вимагачів (Ransomware), GhostLock не шифрує і не знищує дані, а діє як атака на відмову в обслуговуванні (DoS). Загроза зникає після примусового завершення сесії зловмисника або перезавантаження системи.

**Простими словами (Оцінка ризику)** Хакерам більше не обов'язково розгортати складні віруси для шифрування, щоб зупинити роботу установи. Зловмисник, маючи доступ до звичайного облікового запису працівника, може масово "зайняти" всі ключові документи на спільному мережевому диску. Для об'єктів критичної інфраструктури (ОКІ) та закладів охорони здоров'я це означає раптову неможливість доступу до баз даних, фінансових звітів або службових реєстрів в інформаційно-комунікаційних системах (ІКС). Оскільки атака використовує легітимні функції операційної системи, традиційні антивіруси її не бачать. Такий метод блокування дуже часто використовується як "димова завіса": поки технічні фахівці шукають причину масового збою доступу, хакери непомітно викрадають конфіденційну інформацію з інших сегментів мережі.

**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації доцільно налаштувати моніторинг аномалій на рівні файлових серверів. Необхідно відстежувати різке зростання кількості відкритих файлів з параметром ексклюзивного доступу для однієї сесії користувача (SMB-з'єднання). Оскільки ця активність не фіксується у звичайних подіях Windows, для виявлення слід інтегрувати телеметрію платформ керування сховищами із системами SIEM або засобами мережевого аналізу (NDR).
2. **Відповідність нормативним вимогам**
   - Захист ресурсів від блокування доступу та забезпечення безперервного моніторингу мережі відповідають вимогам Наказу ДССЗІ № 75, зокрема функціям «Виявлення» (категорія DE.CM-01: Мережевий моніторинг) та «Захист» (категорія PR.PT-04: Захист від відмови в обслуговуванні). Впровадження інструментів проактивного виявлення аномалій є базовою складовою підтримки цільового профілю безпеки в рамках системи управління ризиками (RMF) та збереження Авторизації систем згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується переглянути та жорстко регламентувати права доступу до спільних мережевих ресурсів (SMB-тек) за принципом найменших привілеїв. Керівникам установ варто затвердити оновлені Стандартні операційні процедури (СОП) щодо реагування на масове блокування файлів, які мають включати алгоритм швидкого примусового завершення аномальних сесій (kill session) без необхідності повного перезавантаження критичних серверів.

**Додаткові матеріали**

- BleepingComputer: New GhostLock tool abuses Windows API to block file access — https://www.bleepingcomputer.com/news/security/new-ghostlock-tool-abuses-windows-api-to-block-file-access/

# Управління доступом — Концепція Device Trust як критичний елемент архітектури Нульової Довіри (Zero Trust)


**Суть оновлення** Аналітики Specops Software та статистичні дані Verizon DBIR підтверджують, що компрометація ідентифікаційних даних фігурує у 44.7% випадків успішних кібератак. Сучасні фішингові інструментарії (зокрема класу AiTM — Adversary-in-the-Middle) навчилися повністю обходити багатофакторну автентифікацію (MFA) шляхом перехоплення сесійних токенів (cookie) безпосередньо у процесі логіна. Оскільки вкрадений токен у браузері хакера виглядає ідентично легітимному, класичні журнали автентифікації не здатні зафіксувати аномалію. Фундаментальні вимоги Zero Trust (зокрема стандарт NIST SP 800-207) наголошують: перевірка ідентичності користувача без урахування поточного стану безпеки його пристрою (Device Posture) створює критичну "сліпу зону" після проходження авторизації.

**Простими словами (Оцінка ризику)** Класичний підхід "перевірив логін і пароль — пропустив у мережу" більше не спроможний захистити інфраструктуру. Якщо зловмисники перехоплять активну сесію працівника, вони зможуть безперешкодно увійти в систему з будь-якого стороннього ноутбука, і для засобів захисту цей вхід виглядатиме як повністю легітимний. Для установ та об'єктів критичної інфраструктури (ОКІ) це створює загрозу невидимого проникнення всередину периметра. Наявність діючого облікового запису не є гарантією безпеки, якщо підключення здійснюється з незахищеного, нешифрованого або неоновленого пристрою. Це створює прямий ризик витоку службових реєстрів, компрометації конфіденційних даних та тривалого порушення безперервності діяльності (business continuity) установи через можливість прихованого впровадження шкідливого ПЗ.

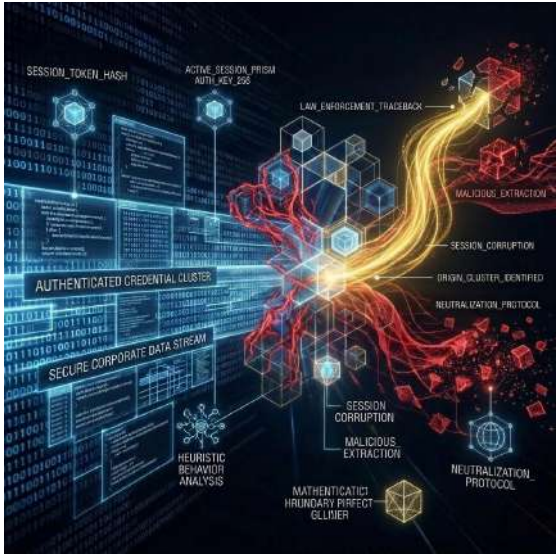
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - ІТ-підрозділам та Підрозділам захисту інформації та кіберзахисту доцільно розгорнути та налаштувати корпоративні політики умовного доступу (Conditional Access). Необхідно заблокувати можливість авторизації у робочих сервісах, пошті та VPN, якщо пристрій не внесено до реєстру довіреного корпоративного обладнання. Доступ має надаватися лише у разі відповідності кінцевої точки базовим критеріям безпекового стану: активний та працездатний EDR/антивірус, увімкнене повне шифрування жорстких дисків (BitLocker/FileVault) та відсутність затримок у встановленні критичних оновлень ОС.
2. **Відповідність нормативним вимогам**
   - Обмеження доступу з неперевірених пристроїв та жорсткий контроль конфігурацій кінцевих точок прямо відповідають вимогам Наказу ДССЗІ № 75, зокрема функціям управління мобільними пристроями та конфігураціями (PR.PT-01: Управління конфігураціями кінцевих пристроїв та PR.PT-03: Управління мобільними пристроями — MDM). Інтеграція контексту безпеки заліза в процеси авторизації є обов'язковим фундаментом для підтримання цільового профілю безпеки в рамках ризик-орієнтованого підходу (RMF) та безперервної Авторизації систем за Постановою КМУ № 712.
3. **Стратегічне планування**
   - Рекомендується розробити та затвердити внутрішні Стандартні операційні процедури (СОП), які повністю забороняють доступ до службових ІКС із некерованого або особистого обладнання працівників (BYOD) без встановлених агентів контролю комплаєнсу. Стратегічний фокус безпеки має бути зміщений з одноразової перевірки пароля на етапі входу до безперервного моніторингу пристрою протягом усієї сесії. У разі відключення засобів захисту чи деградації безпеки заліза mid-session, система повинна автоматично обривати сесію або обмежувати права. Керівникам установ варто ініціювати впровадження інструментів самостійного усунення невідповідностей користувачами (self-service remediation), щоб співробітники могли оперативно оновити ОС чи увімкнути антивірус за інструкцією без залучення технічної підтримки та створення інцидентів.

**Додаткові матеріали**

- BleepingComputer: Identity Alone Isn't Enough: Why Device Security Has to Share the Load — https://www.bleepingcomputer.com/news/security/identity-alone-isnt-enough-why-device-security-has-to-share-the-load

# Протидія кіберзлочинності — Українська кіберполіція викрила масштабну мережу викрадення ідентифікаційних даних (Infostealer)




**Суть оновлення** Кіберполіція України у співпраці з правоохоронними органами США викрила 18-річного підозрюваного з Одеси, який адміністрував масштабну інфраструктуру для розповсюдження шкідливого ПЗ класу Infostealer. Протягом 2024–2025 років зловмисники інфікували пристрої користувачів, викрадаючи облікові дані, файли cookie та сесійні токени. У результаті було скомпрометовано близько 28 000 облікових записів, понад 5 800 з яких використано для несанкціонованих фінансових транзакцій на суму $721 000. Вкрадені сесійні дані, що дозволяють обходити перевірки багатофакторної автентифікації (MFA), реалізовувалися через тіньові онлайн-ресурси та Telegram-боти. В ході обшуків правоохоронці вилучили цифрові докази, серверну аналітику та доступи до криптогаманців.

**Простими словами (Оцінка ризику)** Ця успішна операція української кіберполіції підсвічує критичний вектор атак — використання вірусів типу Infostealer. Головна небезпека полягає в тому, що такі програми викрадають не лише логіни й паролі, а й активні сесійні токени браузера. Це дозволяє зловмисникам «клонувати» поточну робочу сесію працівника і заходити в корпоративні системи, повністю обходячи багатофакторну автентифікацію (MFA). Для державних установ та об'єктів критичної інфраструктури (ОКІ) інфікування навіть одного робочого комп'ютера таким вірусом створює ризик непомітного отримання доступу до внутрішніх інформаційно-комунікаційних систем (ІКС). Зрештою це може призвести до масштабної компрометації службових реєстрів та тривалого порушення безперервності діяльності (business continuity) без жодного попередження для систем безпеки.

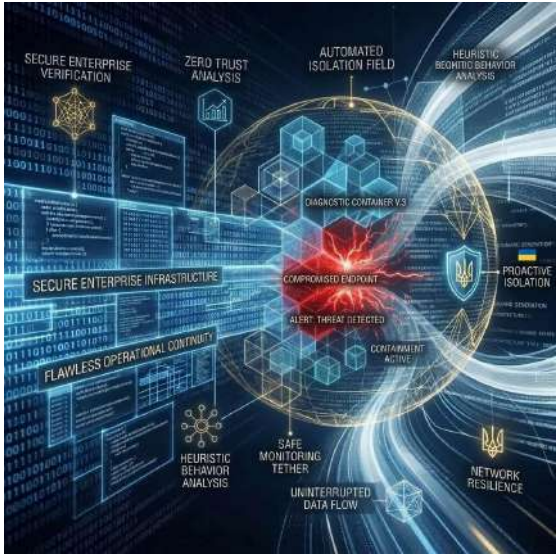
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - Підрозділам захисту інформації та кіберзахисту доцільно налаштувати корпоративні браузери та системи єдиного входу (SSO) на використання короткострокових сесійних токенів та їх примусове анулювання у разі зміни IP-адреси або контексту пристрою. Також варто посилити технічний контроль за встановленням сторонніх розширень у браузерах та блокувати запуск неперевірених виконуваних файлів, які найчастіше є носіями Infostealer-вірусів.
2. **Відповідність нормативним вимогам**
   - Захист від шкідливого ПЗ та контроль засобів автентифікації безпосередньо відповідають вимогам Наказу ДССЗІ № 75, зокрема заходам PR.PT-02 (Запровадження механізмів захисту від шкідливого коду) та PR.AC-07 (Використання стійкої автентифікації). Систематичне виконання цих вимог є обов'язковим для підтримання цільового профілю безпеки в межах переходу на систему управління ризиками (RMF) та успішної Авторизації ІКС згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - ІТ-підрозділам рекомендується розробити та впровадити Стандартні операційні процедури (СОП) щодо регулярного моніторингу тіньових ресурсів на предмет витоку корпоративних облікових даних установи. Керівникам закладів охорони здоров'я варто звернути увагу на успішний досвід українських правоохоронців і пам'ятати, що оперативна взаємодія з державними органами (зокрема своєчасна передача індикаторів компрометації) є ключем до ефективної та комплексної протидії сучасним загрозам.

**Додаткові матеріали**

- BleepingComputer: Ukraine identifies infostealer operator tied to 28,000 stolen accounts — https://www.bleepingcomputer.com/news/security/ukraine-identifies-infostealer-operator-tied-to-28-000-stolen-accounts/

# Автоматизація реагування — Microsoft Defender автоматично ізолює скомпрометовані пристрої




**Суть оновлення** Компанія Microsoft наразі тестує (у режимі попереднього перегляду) нову функціональність для платформи Microsoft Defender for Endpoint, яка здатна автоматично ізолювати скомпрометовані кінцеві точки від корпоративної мережі. Цей механізм є частиною функції автоматичного переривання атак (automatic attack disruption), що розроблена для стримування загроз, обмеження їхнього впливу та надання командам безпеки додаткового часу на розслідування інцидентів. Ізольований пристрій повністю відключається від загальної мережі, але зберігає захищений зв'язок зі службою Defender for Endpoint для безперервного моніторингу та збору телеметрії. Функція працює для робочих станцій, які підключені (onboarded) та керуються через Microsoft Defender for Endpoint, а технічні спеціалісти можуть зняти ізоляцію вручну після усунення ризиків.

**Простими словами (Оцінка ризику)** Коли хакери отримують первинний доступ до одного комп'ютера працівника закладу охорони здоров'я чи об'єкта критичної інфраструктури (OKI), їхня наступна мета — швидко переміститися внутрішньою мережею (lateral movement) до критичних баз даних чи серверів. Якщо блокування інфікованого пристрою виконується вручну, цей процес може зайняти критично важливі хвилини, що створює ризик масового поширення вірусів-вимагачів (Ransomware) або витоку конфіденційної інформації. Автоматична ізоляція діє як миттєвий і точний «карантин»: комп'ютер миттєво відрізається від інфраструктури, блокуючи дії хакера, але залишається доступним для IT-фахівців для аналізу. Це дозволяє зберегти безперервність діяльності (business continuity) всієї установи, локалізувавши проблему виключно на рівні одного скомпрометованого вузла.

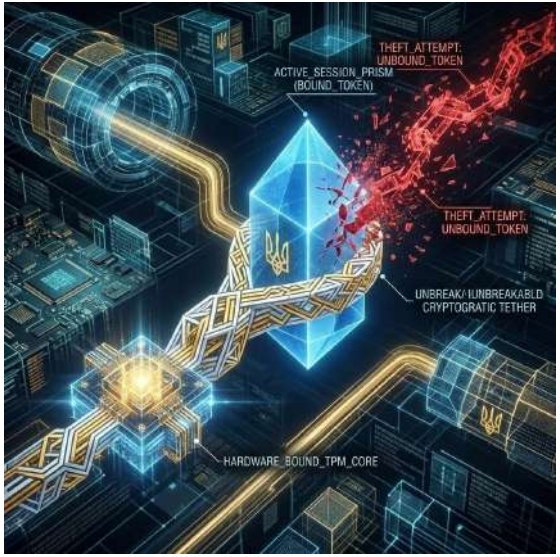
**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - IT-підрозділам та Підрозділам захисту інформації та кіберзахисту доцільно перевірити налаштування корпоративних систем захисту кінцевих точок (EDR/XDR) та активувати механізми автоматичного переривання атак (за наявності відповідних ліцензій). Варто переконатися, що всі критично важливі робочі станції коректно підключені до централізованої системи управління (onboarded), щоб у разі інциденту ізоляція спрацювала миттєво.
2. **Відповідність нормативним вимогам**
   - Впровадження автоматизованих інструментів стримування кіберінцидентів безпосередньо відповідає вимогам Наказу ДССЗІ № 75, зокрема заходам із функції «Реагування» (категорія RS.MI-01: Стримування інцидентів та категорія RS.MI-02: Ізоляція скомпрометованих систем). Використання сучасних рішень класу EDR є важливою складовою підтримки цільового профілю безпеки та ефективного впровадження системи управління ризиками (RMF), що є обов'язковою умовою для проходження Авторизації ІКС згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - Рекомендуємо актуалізувати внутрішні Стандартні операційні процедури (СОП) щодо реагування на кіберінциденти. У них варто детально прописати алгоритми дій адміністраторів під час автоматичного спрацювання ізоляції (зокрема, як аналізувати зібрану телеметрію та за яких умов безпечно знімати блокування через панель управління). Керівникам державних установ доцільно розглянути стратегічну модернізацію базових антивірусів до проактивних систем, здатних автоматизувати процеси безпеки та зменшити навантаження на профільних фахівців.

**Додаткові матеріали**

- BleepingComputer: Microsoft Defender can now automatically isolate hacked endpoints — https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-can-now-automatically-isolate-hacked-endpoints/

# Захист ідентифікації — Google Chrome блокує викрадення сесійних токенів завдяки апаратній прив'язці




**Суть оновлення** Компанія Google розгортає для всіх користувачів (зокрема клієнтів Google Workspace) нову функцію проактивної безпеки — Device Bound Session Credentials (DBSC). Ця технологія криптографічно прив'язує сесійні файли cookie безпосередньо до апаратного модуля безпеки комп'ютера (наприклад, чипа TPM у середовищі Windows або Secure Enclave у macOS). Оскільки унікальні ключі шифрування формуються на апаратному рівні і не можуть бути вилучені з мікрочипа, зловмисники втрачають можливість використовувати викрадені cookie-файли для обходу багатофакторної автентифікації (MFA) та перехоплення облікових записів. Для корпоративних клієнтів Google Workspace функція вмикається за замовчуванням, і адміністратори не можуть її вимкнути. Зазначається, що це кардинально змінює підхід: від реактивного виявлення до проактивного запобігання крадіжкам.

**Простими словами (Оцінка ризику)** Раніше існувала критична проблема: віруси класу Infostealer (такі як Lumma чи Rhadamanthys) могли вкрасти "зліпок" активної сесії з браузера працівника і передати його хакеру. Маючи такий "зліпок", зловмисник міг зайти в корпоративну систему без введення пароля чи підтвердження MFA з будь-якого іншого пристрою. Тепер Google зробив так, що сесійний токен фізично "прив'язаний" до "заліза" конкретного комп'ютера. Навіть якщо вірус викраде файл cookie, він перетвориться на марний набір даних на комп'ютері зловмисника, оскільки там немає потрібного апаратного чипа. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) це суттєво зменшує ризики несанкціонованого доступу до інформаційно-комунікаційних систем (ІКС) та захищає безперервність діяльності (business continuity) від наслідків успішного фішингу.

**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - ІТ-підрозділам доцільно переконатися, що на всіх корпоративних робочих станціях активовані модулі довіреної платформи (TPM 2.0). Окрім того, необхідно забезпечити централізоване оновлення браузерів Google Chrome до актуальних версій, щоб механізм DBSC працював коректно та покривав усі активні сесії працівників.
2. **Відповідність нормативним вимогам**
   - Використання апаратних засобів для захисту автентифікаційних даних прямо відповідає вимогам Наказу ДССЗІ № 75, зокрема заходу PR.PT-06 (Встановлення та використання заходів безпеки, що базуються на апаратному забезпеченні). Реалізація цього контролю є невід'ємною частиною підтримки цільового профілю безпеки в рамках системи управління ризиками (RMF) та сприяє успішному проходженню Авторизації ІКС згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - Підрозділам захисту інформації та кіберзахисту рекомендується впровадити політики корпоративного управління браузерами (Enterprise Browser Management). Це дозволить примусово активувати додаткові рівні захисту (наприклад, режим Enhanced Safe Browsing для протидії фішингу та шкідливому ПЗ), а також стандартизувати налаштування безпеки на всіх пристроях установи згідно із затвердженими СОПами.

**Додаткові матеріали**

- BleepingComputer: Google Chrome adds session cookie theft protection for all users — https://www.bleepingcomputer.com/news/security/google-chrome-adds-session-cookie-theft-protection-for-all-users/

# Захист ідентифікації — Оновлення парольних політик в Active Directory без шкоди для користувачів


**Суть оновлення** Паролі, створені за застарілими вимогами до складності — із примусовим поєднанням цифр, спеціальних символів, великих та малих літер (наприклад, `P@ssw0rd!`) більше не забезпечують належного рівня захисту та часто призводять до повторного використання або записування паролів на папірцях. Експерти з кібербезпеки та NIST (Національний інститут стандартів і технологій США) рекомендують переходити до використання "парольних фраз" (passphrases) — довгих комбінацій звичайних слів (до 64 символів), які легше запам'ятати, але математично набагато складніше зламати. Також наголошується на важливості автоматичного блокування паролів, які вже були скомпрометовані у відомих витоках баз даних (breached credentials), за допомогою спеціалізованих рішень, таких як Specops Password Policy. Сучасні стандарти пропонують відмовитися від регулярної (наприклад, щомісячної) примусової зміни паролів, оскільки це лише стимулює користувачів створювати слабкі, передбачувані варіації одного й того ж пароля.

**Простими словами (Оцінка ризику)** Коли ми змушуємо лікарів чи бухгалтерів щомісяця вигадувати новий пароль із великими літерами, цифрами та спецсимволами, вони просто додають 1, 2 або ! до старого пароля. Хакери чудово знають про ці звички і використовують автоматизовані атаки (password spraying), щоб "пробити" захист. Для державних установ та об'єктів критичної інфраструктури (ОКІ) слабкий або скомпрометований пароль у корпоративній системі Active Directory (AD) — це відкриті двері для зловмисників. Якщо вони отримають доступ до AD, то зможуть контролювати всю мережу закладу охорони здоров'я, що загрожує не лише витоком даних, а й повною зупинкою інформаційно-комунікаційних систем (ІКС) через розгортання вірусів-вимагачів.

**Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)**

1. **Практичний крок:**
   - ІТ-підрозділам доцільно переглянути налаштування групових політик (GPO) для Active Directory. Рекомендується збільшити мінімальну довжину пароля (наприклад, до 15 символів), але при цьому дозволити використання простіших, легко запам'ятовуваних парольних фраз. Також варто розглянути можливість впровадження корпоративного менеджера паролів та налаштування порталу самообслуговування (Self-Service Password Reset), що дозволить співробітникам безпечно скидати паролі без залучення технічної підтримки.
2. **Відповідність нормативним вимогам**
   - Застосування надійних парольних політик є прямою вимогою Наказу ДССЗІ № 75 (функція "Ідентифікація", категорія "Контроль доступу" — PR.AC-06: Застосування принципу найменших привілеїв та керування ідентифікаторами). Відмова від використання скомпрометованих паролів та перехід до сучасних стандартів автентифікації є необхідною умовою для забезпечення цільового профілю безпеки в рамках системи управління ризиками (RMF) та підтримки статусу Авторизації систем відповідно до Постанови КМУ № 712.
3. **Стратегічне планування**
   - Керівникам установ варто ініціювати розробку оновлених Стандартних операційних процедур (СОП) щодо управління паролями. Доцільно впровадити рішення, які перевіряють корпоративні паролі за базами відомих витоків у режимі реального часу, щоб блокувати використання скомпрометованих даних ще на етапі створення облікового запису. Окрім того, важливо запровадити "динамічне старіння паролів", коли термін дії пароля залежить від його довжини: чим довший пароль, тим рідше його потрібно змінювати.

**Додаткові матеріали**

- BleepingComputer: Can you enforce strong Active Directory password rules without frustrating users? — https://www.bleepingcomputer.com/news/security/can-you-enforce-strong-active-directory-password-rules-without-frustrating-users/