МІНІСТЕРСТВО ОБОРОНИ ПІДПРИЄМСТВО УКРАЇНИ

Кібер-дайджест МОЗ України

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

Лютий 2026

Нормативні оновлення — Розширення переліку забороненого ПЗ та обладнання

Суть оновлення Адміністрація Держспецзв'язку (ДССЗІ) внесла 13 нових позицій до офіційного відкритого переліку програмного забезпечення та комунікаційного (мережевого) обладнання, забороненого до використання в органах державної влади та на об'єктах критичної інфраструктури (відповідно до постанови КМУ від 22.10.2025 № 1335).

Простими словами (Оцінка ризику) Держава регулярно оновлює список "токсичних" програм та мережевого обладнання, які містять приховані вразливості або контролюються ворожими спецслужбами. Наявність таких апаратних чи програмних рішень у мережі установи — це гарантований канал витоку службової інформації. Використання заборонених рішень дозволяє зловмисникам непомітно шпигувати за мережею або дистанційно зупинити роботу критичних систем закладу. Крім того, ігнорування цього переліку є прямим порушенням вимог законодавства у сфері захисту інформації.

Заходи з нейтралізації та комплаєнсу (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

1. **Позачергова звірка та інвентаризація активів**
   - **Дія:** Відповідальним фахівцям завантажити актуальний перелік із сайту ДССЗІ та провести звірку наявного в установі програмного та апаратного забезпечення. Це безпосередньо закриває вимоги пунктів **ID.AM-01** (інвентаризація обладнання) та **ID.AM-02** (інвентаризація ПЗ) Базових заходів з кіберзахисту.
   - **Обґрунтування:** Системне виявлення активів, використання яких створює неприпустимі ризики для інфраструктури, є базовим етапом управління ризиками.
2. **Ізоляція та виведення з експлуатації**
   - **Дія:** У разі виявлення заборонених позицій — негайно ізолювати відповідне обладнання від локальної мережі та інтернету, деінсталювати заборонене ПЗ та розпочати процедуру їх планової заміни на безпечні аналоги.
   - **Обґрунтування:** Унеможливлення використання вбудованих бекдорів для проведення диверсій або збору розвідувальних даних всередині периметра установи.
3. **Коригування процедур публічних закупівель**
   - **Дія:** Зобов'язати IT-підрозділи/Підрозділи захисту інформації спільно з тендерними комітетами перевіряти технічні специфікації на предмет відсутності рішень із переліку ДССЗІ до моменту оголошення закупівель.
   - **Обґрунтування:** Запобігання нецільовому використанню бюджетних коштів та уникнення юридичної відповідальності за закупівлю санкційного обладнання.

Додаткові матеріали

- Офіційний ресурс: Перелік забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання (Сайт Держспецзв'язку)

Державна політика — Результати реалізації Стратегії кібербезпеки України у 2025 році

Суть оновлення Держспецзв'язку оприлюднила звіт, згідно з яким рівень реалізації заходів Стратегії кібербезпеки України за минулий рік сягнув 86%. Попри активні бойові дії та постійні кібератаки, ключові завдання у сферах стримування ворога та забезпечення кіберстійкості критичної інфраструктури були виконані.

Простими словами (Оцінка ризику) Національна система кібербезпеки перейшла від режиму «екстреного реагування» до системної розбудови захисту. Високий показник виконання Стратегії означає, що державні органи та об'єкти критичної інфраструктури (ОКІ) переходять на єдині європейські стандарти безпеки. **Для наших установ** це сигнал, що кіберзахист більше не є факультативним питанням — це обов'язкова складова функціонування держави. Будь-яка невідповідність локальних заходів захисту загальнодержавним вимогам створює «слабку ланку», через яку ворог може атакувати всю цифрову екосистему країни.

Заходи з посилення спроможностей (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

1. **Актуалізація планів кіберзахисту установ**
   - **Дія:** Використовувати результати звіту як базу для перегляду та актуалізації внутрішніх планів кіберзахисту. Особливу увагу приділити розділам щодо виявлення та відновлення (RC.RP) після інцидентів.
   - **Обґрунтування:** Стратегічний підхід вимагає від кожної установи наявності чіткого алгоритму дій, що корелюється із національними пріоритетами кіберстійкості.
2. **Підготовка до масштабних тренувань та навчань**
   - **Дія:** Включити до графіку роботи персоналу IT-підрозділів/Підрозділів захисту інформації участь у галузевих кібернавчаннях (на базі CERT-UA або ДССЗІ).
   - **Обґрунтування:** Звіт підтверджує, що навчання персоналу є ключовим чинником успішного відновлення систем після атак. Практичні навички фахівців у регіонах — це запорука безперервності надання послуг.
3. **Імплементація технічних стандартів взаємодії**
   - **Дія:** Забезпечити технічну готовність до обміну даними про кіберінциденти з національними центрами (CERT-UA). Перевірити наявність та працездатність інструментів збору логів (Log Management) та систем моніторингу в мережах установ.
   - **Обґрунтування:** Посилення взаємодії — один із трьох стратегічних напрямів держави. Оперативна передача індикаторів компрометації дозволяє захистити інші заклади охорони здоров'я від аналогічних атак.

Додаткові матеріали

- Офіційний ресурс: Аналітичний звіт про стан виконання Стратегії (Сайт ДССЗІ)

Новий порядок реагування — Від реакції до проактивного захисту (Наказ № 143)

Суть оновлення Адміністрація Держспецзв'язку затвердила **Наказ від 18.02.2026 № 143**, який впроваджує сучасний ризикоорієнтований підхід до реагування на кіберінциденти. Основна зміна — перехід від «гасіння пожеж» до **проактивного управління загрозами**. Впроваджено п'ятибальну шкалу критичності (від «білого» до «чорного» рівня) та уніфіковану форму повідомлення про інцидент, що дозволяє командам CERT-UA реагувати миттєво.

Простими словами (Оцінка ризику) Уявіть це як медичне сортування (тріаж) у приймальному відділенні. Раніше ми повідомляли про «хворобу» (злам), коли система вже «не дихала». Новий підхід вимагає моніторити «симптоми» (кіберзагрози) заздалегідь. Головне правило тепер: **спочатку повідомити про факт атаки**, а технічні деталі додавати потім. Це дозволяє фахівцям CERT-UA або галузевим центрам розпочати допомогу вашій установі на годину-дві раніше, що в кіберсвіті часто вирішує долю всіх даних закладу.

Рекомендовані напрями для опрацювання (Для IT-підрозділів / Підрозділів захисту інформації)

1. **Практичне налаштування через GPO (Швидкий доступ до допомоги)**
   - **Пропозиція:** Розгорнути на робочих столах усіх працівників установи ярлик або «тривожну кнопку» для швидкого доступу до внутрішньої форми повідомлення про інцидент.
   - **Шлях GPO:** `User Configuration -> Preferences -> Windows Settings -> Shortcuts`.
   - **Дія:** Створити ярлик, що веде на внутрішній ресурс із **Уніфікованою формою повідомлення** (згідно з Наказом № 143). Це забезпечить збір первинної технічної інформації (час, сектор, об'єкти впливу) безпосередньо від свідка події.
2. **Відповідність вимогам Наказу № 75 (Планування реагування)**
   - **Пункт: RS.MA-01 (Управління кіберінцидентами — Виконання плану реагування) або ID.IM-04 (Удосконалення — Розробка та перегляд плану реагування).**
   - **Обґрунтування:** Оновлення внутрішніх регламентів установи відповідно до чотирьох етапів (Підготовка, Виявлення, Стримування, Пост-інцидентний аналіз) прямо відповідає вимогам Наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту».
3. **Впровадження протоколу TLP для обміну даними (Порада фахівця)**
   - **Пропозиція:** Навчити персонал підрозділу захисту інформації використовувати маркування **TLP (Traffic Light Protocol)** при передачі даних про інциденти.
   - **Дія:** Використовуйте `TLP:RED` для інформації, що не має виходити за межі групи реагування, та `TLP:AMBER` для обмеженого поширення всередині установи. Це гарантує, що конфіденційні деталі про вразливості вашої мережі не стануть відомі стороннім особам під час обміну інформацією.

Додаткові матеріали

- Текст Наказу та нові чеклісти: Офіційний сайт Держспецзв'язку

Тренди кіберзагроз та допомога CERT-UA — Головне з Kyiv Cyber Resilience Forum

Суть загрози Кількість кібератак в Україні зросла майже втричі. Угруповання **Gamaredon** (UAC-0010) викрадає до 100 тис. файлів щодня, використовуючи легітимні інструменти Windows, що робить звичайні антивіруси неефективними. **APT28** експлуатує вразливості Microsoft Office вже наступного дня після їх оприлюднення. Також зафіксовано новий тип фішингу — дзвінки через Signal/WhatsApp із використанням ШІ-генерації голосу керівництва.

Простими словами (Оцінка ризику) Ворог став блискавичним: якщо ви не встановили оновлення сьогодні, завтра систему буде зламано. Хакери більше не «ламають» двері — вони використовують «майстер-ключі», вбудовані в саму Windows. Крім того, зловмисники тепер можуть «дзвонити» працівникам голосом головного лікаря чи директора департаменту, щоб виманити паролі. Успіх більшості атак базується на елементарних помилках: відкритих портах та відсутності «загартування» (харденінгу) систем.

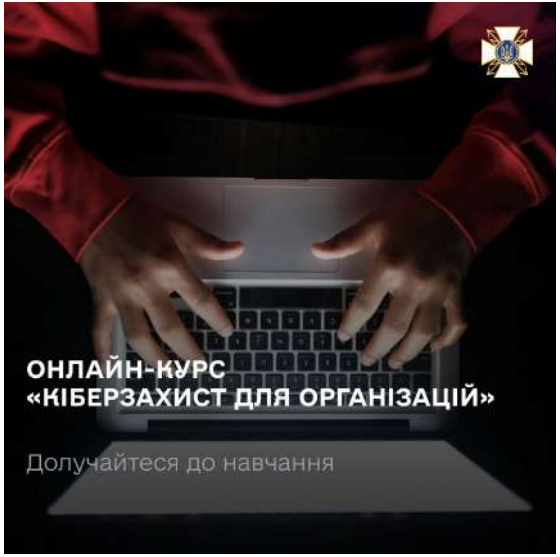
Рекомендовані напрями для опрацювання (Для IT-підрозділів / Підрозділів захисту інформації)

1. **Харднінг систем через GPO (Обмеження інструментів хакера)**
   - **Пропозиція:** Заборонити використання командного рядка (CMD) та PowerShell для звичайних користувачів, які не мають стосунку до адміністрування.
   - **Шлях GPO:** `User Configuration\Administrative Templates\System` -> параметр **Prevent access to the command prompt**.
   - **Дія:** Це заблокує можливість угрупованню наприклад, Gamaredon використовувати легітимні утиліти Windows для закріплення в системі.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Харднінг)**
   - **Пункт: PR.PS-01 (Встановлення та застосування методів керування конфігурацією — Харднінг).**
   - **Обґрунтування:** Впровадження інструкцій із налаштування безпеки ОС та відключення непотрібних служб відповідає вимогам Наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту».
3. **Системна стандартизація та автоматизація (CIS Benchmarks + MISP)**
   - **Пропозиція:** Об'єднати статичний захист конфігурацій (за стандартами **CIS Benchmarks**) із динамічним автоматизованим блокуванням загроз через платформу **MISP**.
   - **Дія:**
     - Використання профілю **CIS Level 1** дозволяє автоматично закрити до 80-90% типових вразливостей налаштувань Windows та браузерів.
     - Інтеграція безкоштовних конекторів від **CERT-UA** для вашого Firewall дозволить мережі автоматично отримувати індикатори компрометації (IoC) та блокувати ворожі сервери ще до початку атаки.
   - **Результат:** Ви створюєте автономний контур безпеки, який потребує мінімального втручання адміністратора.

Додаткові матеріали

- Подробиці виступу: Еволюція кіберзагроз (сайт ДССЗІ)
- Міжнародні стандарти: CIS Benchmarks
- Консультації щодо підключення до MISP: Роз'яснення CERT-UA щодо MISP

Навчання та розвиток персоналу — Онлайн-курс «Кіберзахист для організацій»



Суть оновлення Держспецзв'язку спільно з партнерами актуалізували та масштабували безкоштовний навчальний курс «Кіберзахист для організацій». Програма охоплює практичні аспекти захисту від кібератак, алгоритми реагування на інциденти, технічне налаштування систем захисту та правила кібергігієни для працівників. За останній рік навчання успішно пройшли понад 23 тисячі осіб.

Простими словами (Оцінка ризику) Більшість успішних кібератак починається через людський фактор (відкриття шкідливих посилань, використання слабких паролів, ігнорування протоколів безпеки). Наявність навченого персоналу — це «живий щит» для цифрової інфраструктури установи. Проходження цього курсу дозволяє працівникам не лише отримати теоретичні знання, а й навчитися розпізнавати спроби злому на ранніх етапах, що значно знижує ризик повної зупинки роботи систем через дії користувача.

Заходи з посилення спроможностей (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

1. **Проходження курсу профільними фахівцями**
   - **Дія:** Забезпечити обов'язкове проходження курсу співробітниками IT-підрозділів/Підрозділів захисту інформації установи.
   - **Обґрунтування:** Отримання актуальних знань щодо реагування на інциденти та адміністрування засобів захисту згідно з державними стандартами.
2. **Розробка та проведення локальних навчань з кібергігієни**
   - **Дія:** На основі матеріалів курсу (зокрема розділів про роботу з персоналом) розробити та провести короткі періодичні інструктажі для всіх працівників установи.
   - **Обґрунтування:** Зменшення впливу «людського фактора». Персонал повинен отримувати знання з кібергігієни у зрозумілій формі безпосередньо від своїх технічних спеціалістів.
3. **Спеціалізоване навчання для керівництва установи**
   - **Дія:** Керівникам установи та лідерам структурних підрозділів рекомендується пройти навчання на платформі «StudyiЯ», щоб розуміти стратегічну важливість кіберзахисту в управлінських процесах.
   - **Обґрунтування:** Формування культури безпеки «зверху вниз» та підтримка ініціатив IT-підрозділів/Підрозділів захисту інформації.

Додаткові матеріали

- **Для технічних спеціалістів (Платформа Skovoroda):** Курс «Кіберзахист для організацій»
- **Для державних службовців (Портал StudyiЯ):** Вища школа публічного управління

Галузеві загрози — Ціна бездіяльності та наслідки системної недбалості (Кейс UMMC)

Суть події Медичний центр Університету Міссісіпі (UMMC) зафіксував четверту масштабну кібератаку за три роки. Розслідування виявило, що установа раніше вже сплачувала рекордний штраф у розмірі **2,75 млн доларів** за порушення правил захисту даних. Критичним фактом є те, що керівництво установи знало про вразливості систем ще з 2005 року, але не вживало жодних реальних заходів до моменту виникнення першого великого витоку даних.

Простими словами (Оцінка ризику) Історія UMMC — це наочний приклад того, що «економія» на кіберзахисті призводить до катастрофічних наслідків. Хоча в Україні наразі не застосовуються прямі фінансові санкції такого масштабу, **персональна відповідальність керівника установи** за неналежний захист критичної інфраструктури в умовах війни є надзвичайно високою. Окрім ризику повної зупинки надання медичної допомоги чи критичних послуг, недбалість може призвести до потрапляння конфіденційної інформації до рук ворога, що кваліфікується як загроза національній безпеці. Будь-яка виявлена вразливість має бути усунена планово, а не після того, як стався інцидент.

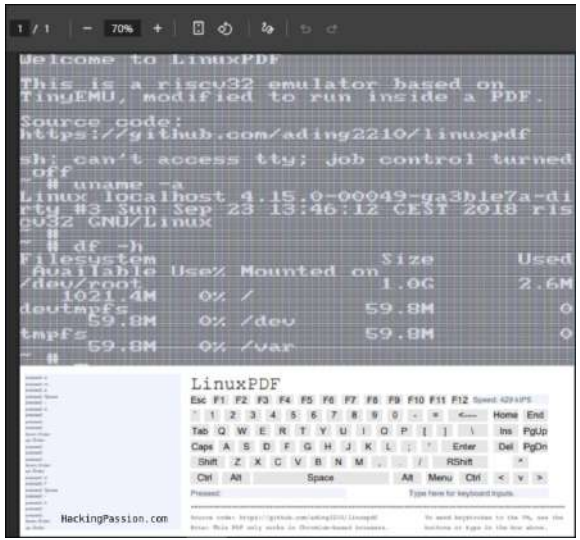
Рекомендовані напрями для опрацювання (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

1. **Планове усунення виявлених невідповідностей**
   - **Пункт:** ID.RA-06 (Визначення заходів реагування на ризики та їх пріоритетність) або PR.PS-02 (Належне обслуговування програмного забезпечення).
   - **Обґрунтування:** Складання графіка усунення вразливостей на основі результатів сканувань та перевірок безпосередньо відповідає вимогам заходу **ID.RA-06** щодо встановлення пріоритетності реагування на ризики та їх обов'язкового відстеження. Також це забезпечує виконання вимог заходу **PR.PS-02** стосовно виправлення вразливостей у чітко визначені планом терміни для мінімізації ризиків. Це здійснюється на виконання Наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту».
2. **Забезпечення фізичної та технічної безпеки кінцевих пристроїв**
   - **Пропозиція:** Розглянути можливість впровадження повного шифрування дисків на ноутбуках установи та регламентувати порядок використання техніки за межами закладу.
   - **Обґрунтування:** Оскільки кейс UMMC почався з крадіжки ноутбука, такий підхід забезпечує виконання вимог щодо захисту даних на мобільних пристроях.
3. **Розробка планів аварійного відновлення (DRP)**
   - **Пропозиція:** Протестувати та регулярно оновлювати плани дій у надзвичайних ситуаціях (Emergency Operations Plan), обов'язково включивши до них технічний **План аварійного відновлення (Disaster Recovery Plan — DRP)**.
   - **Контекст:** План DRP має містити покрокові інструкції для IT-підрозділів / Підрозділів захисту інформації щодо черговості відновлення сервісів (СЕД, пошта, реєстри) та перевірки цілісності бекапів.
   - **Обґрунтування:** Це дозволяє виконати методичні рекомендації щодо забезпечення безперервності діяльності та реагування на інциденти відповідно до Наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75.

Додаткові матеріали

- Деталі розслідування та санкцій: UMMC Data Security Failures and Fines (WLBT News)

Приховані загрози у стандартних документах — Виконання коду через PDF



Суть загрози Дослідники з кібербезпеки продемонстрували запуск повноцінної операційної системи Linux (через емулятор RISC-V TinyEMU) безпосередньо всередині PDF-документа. Запуск відбувається через вбудований у PDF рушій JavaScript при відкритті файлу в браузерах на базі Chromium (Chrome, Edge, Brave тощо).

Простими словами Працівник установи відкриває звичайний на вигляд PDF-файл (наприклад, за посиланням у браузері), і замість статичного тексту прямо всередині документа завантажується та працює повноцінна операційна система. На практиці це означає, що під виглядом стандартного документа (рахунку, резюме чи наказу) зовнішні зловмисники можуть приховати програму для непомітного виконання шкідливого коду одразу після кліку. Крім того, внутрішній порушник (інсайдер) може використати такий файл, щоб отримати неконтрольований термінал Linux та запускати власні команди чи утиліти в мережі установи, обходячи корпоративні заборони на встановлення програмного забезпечення.

Оцінка ризику Документи формату PDF традиційно сприймаються користувачами як безпечні. Проте специфікація PDF дозволяє виконувати складну обчислювальну логіку. В умовах кібервійни ця архітектурна особливість перетворює звичайний файл на плацдарм для обходу базових антивірусних перевірок та потенційного закріплення у внутрішній мережі установи.

Заходи з нейтралізації та посилення безпеки (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

1. **Блокування виконання сценаріїв (JavaScript) у PDF-рідерах**
   - **Дія:** Примусово вимкнути підтримку JavaScript у всіх локальних програмах для читання PDF (наприклад, Adobe Acrobat Reader, Foxit) на робочих станціях.
   - **Обґрунтування:** Мінімізація поверхні атаки. Відключення активного вмісту позбавляє зловмисників основного інструментарію для експлуатації вразливостей без впливу на можливість перегляду тексту працівниками установи.
2. **Ізоляція та контроль вкладень на рівні поштового шлюзу**
   - **Дія:** Налаштувати правила фільтрації вхідної пошти на виявлення та блокування PDF-документів, що містять вбудовані скрипти (JS/ActiveX). За можливості — впровадити технологію очищення контенту (Content Disarm and Reconstruction).
   - **Обґрунтування:** Превентивне блокування вектору атаки до того, як фішинговий лист потрапить до поштової скриньки працівника установи.
3. **Заборона відкриття PDF-файлів вбудованими засобами браузера (Налаштування GPO)**
   - **Політика:** 1.2.6 (L1) Ensure 'Always open PDF files externally' is set to 'Enabled' - за CIS Benchmarks
   - **Налаштування:** `Download PDF files instead of automatically opening them in Chrome`.
   - **Шлях GPO:** `Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\`
   - **Рекомендоване значення:** `Enabled`.
   - **Обґрунтування:** Вбудовані PDF-плагіни браузерів є популярною мішенню для експлойтів. Відкриття файлу зовнішніми програмами дозволяє системним засобам захисту (EDR/Антивірусам) ефективніше ізолювати середовище, сканувати об'єкт та блокувати аномальні процеси в оперативній пам'яті комп'ютера.

Додаткові матеріали

- Детальний технічний розбір: Linux Inside a PDF (Hacking Passion)

Компрометація робочих місць — Шкідливі розширення під виглядом ШІ-помічників

Суть загрози Виявлено масштабну кампанію **AiFrame**, у межах якої понад 30 шкідливих розширень для браузера Chrome (маскувалися під Gemini AI, ChatGPT Sidebar, AI GPT тощо) викрадали облікові дані та вміст електронної пошти користувачів. Загальна кількість інсталяцій перевищила 300 000. Шкідливий код дозволяє зловмисникам зчитувати вміст сторінок, перехоплювати дані автентифікації та повністю копіювати листування в Gmail (включаючи чернетки).

Простими словами (Оцінка ризику) Працівники установ, бажаючи полегшити роботу з документами чи перекладом, самостійно встановлюють "помічники" з магазину Chrome. Проте замість реального сервісу вони отримують шпигунську програму. Оскільки розширення працює безпосередньо в браузері, воно бачить усе, що бачить користувач: паролі до внутрішніх систем, вміст службового листування та персональні дані. Це створює критичний канал витоку інформації за межі захищеного периметра установи.

Заходи з нейтралізації та посилення безпеки (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

Впровадити жорстку політику керування браузерами через групові політики (GPO) для мінімізації ризику встановлення несанкціонованого ПЗ (згідно CIS Benchmarks):

1. **Заборона встановлення зовнішніх розширень (GPO 2.3.1)**
   - **Дія:** Увімкнути політику `Blocks external extensions from being installed`.
   - **Шлях:** `Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\`
   - **Мета:** Заблокувати автоматичне встановлення розширень сторонніми інсталяторами або файлами реєстру без відома користувача.
2. **Обмеження типів дозволених додатків (GPO 2.3.2)**
   - **Дія:** Явно дозволити лише типи розширень, необхідні для роботи, та заблокувати інші.
   - **Шлях GPO:** `Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\`
   - **Налаштування:** `Configure allowed app/extension types`.
   - **Рекомендоване значення:** `Enabled` та додати до списку: `extension`, `hosted_app`, `platform_app`, `theme`.
   - **Мета:** Заборонити використання застарілих або небезпечних типів додатків, які можуть мати надлишкові дозволи та збільшувати поверхню атаки.
3. **Впровадження стратегії «білих списків» (GPO 2.3.3 та 2.3.3.A)**
   - **Дія 1:** Увімкнути `Configure extension installation blocklist` (Шлях: `...Google\Google Chrome\`) зі значенням `*` (блокувати все).
   - **Дія 2:** Через політику `Configure extension installation allowlist` (Шлях: `...Google\Google Chrome\Extensions\`) дозволити лише той перелік ID розширень, який є критично необхідним для роботи установи.
   - **Обґрунтування:** Це реалізує принцип «заборонено все, крім явно дозволеного», запобігаючи встановленню працівниками випадкових шкідливих додатків.

Додаткові матеріали

- Перелік індикаторів компрометації та шкідливих ID: Fake AI Chrome extensions steal credentials (BleepingComputer)

Критична вразливість Chrome — Перший Zero-Day 2026 року (CVE-2026-2441)

Суть загрози Компанія Google випустила екстрене оновлення для браузера Chrome, щоб усунути вразливість високого рівня критичності (CVE-2026-2441, оцінка CVSS: 8.8). Проблема пов'язана з помилкою керування пам'яттю (use-after-free) у системі рендерингу шрифтів. Згідно з даними Google, вразливість уже активно експлуатується в реальних атаках («in the wild»).

Простими словами (Оцінка ризику) Браузер — це основний робочий інструмент кожного працівника установи та головне «вікно» для входу зловмисників. Ця вразливість дозволяє хакерам отримати контроль над комп'ютером працівника просто після того, як він відвідає спеціально створену шкідливу вебсторінку. Жодної іншої дії (завантаження файлів чи натискання кнопок) не потрібно. Оскільки загроза вже використовується для шпигунства та викрадення даних, ігнорування оновлень створює прямий ризик компрометації всієї мережі установи.

Заходи з нейтралізації та посилення безпеки (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

Необхідно негайно переконатися, що браузери оновлені до версії **145.0.7632.75/.76** (Windows, macOS) або **144.0.7559.75** (Linux), та налаштувати примусові політики оновлення через GPO (згідно CIS Benchmarks):

1. **Примусове автоматичне оновлення (GPO 2.1.1)**
   - **Налаштування:** `Update policy override`.
   - **Шлях:** `Computer Configuration\Policies\Administrative Templates\Google\Google Update\Applications\Google Chrome\`
   - **Значення:** `Enabled` (Always allow updates / Automatic silent updates).
   - **Мета:** Гарантувати, що Chrome завжди отримує виправлення безпеки без втручання користувача
2. **Контроль періоду перевірки та сповіщень (GPO 2.1.2 та 2.19)**
   - **Дія 1:** Встановити `Auto-update check period override` на інтервал 5 годин (замість «0»).
   - **Дія 2:** Встановити `Set the time period for update notifications` у значення `86400000` (24 години).
   - **Шлях:** `...Google\Google Chrome\`
   - **Мета:** Забезпечити оперативне виявлення нових патчів та надати користувачеві рівно один день на перезапуск браузера для застосування оновлення.
3. **Оновлення компонентів безпеки (GPO 1.15)**
   - **Налаштування:** `Enable component updates in Google Chrome`.
   - **Шлях:** `...Google\Google Chrome\`
   - **Значення:** `Enabled`.
   - **Мета:** Дозволити Chrome автоматично оновлювати внутрішні модулі захисту (списки відкликаних сертифікатів, Safe Browsing) незалежно від версії самого браузера.

Додаткові матеріали

- Подробиці про вразливість: Google Releases Emergency Patch for Chrome Zero-Day

Таргетований фішинг та віддалений контроль — Активність угруповання UAC-0050 (DaVinci Group)

Суть загрози Угруповання UAC-0050 (також відоме як DaVinci Group), яке пов'язують із **російськими спецслужбами**, розширило географію атак. Зловмисники використовують техніку **Spear-Phishing** (цільовий фішинг), розсилаючи листи нібито від судових органів або державних установ. Мета — встановлення програм **Remote Manipulator System (RMS)** або **RemcosRAT** для повного дистанційного керування комп'ютером жертви, викрадення фінансової документації та паролів.

Простими словами (Оцінка ризику) Зловмисники полюють на конкретних працівників: бухгалтерів, юристів та фахівців із закупівель. Вони надсилають лист, який виглядає як офіційний запит від суду чи контролюючого органу. Усередині — архів із файлом, що має подвійне розширення (наприклад, `Документ.pdf.exe`). Якщо працівник запустить такий файл, хакери отримають такий самий доступ до комп'ютера, як і системний адміністратор: вони зможуть бачити екран, копіювати файли та керувати банківськими рахунками установи. Використання легітимних програм віддаленого доступу (як-от RMS) дозволяє їм залишатися непоміченими для звичайних антивірусів.

Рекомендовані напрями для опрацювання (Для IT-підрозділів / Підрозділів захисту інформації)

1. **Блокування програм несанкціонованого віддаленого доступу**
   - **Пропозиція:** Провести аудит та заблокувати запуск сторонніх засобів віддаленого керування, таких як **RMS (Remote Manipulator System)**, **LiteManager**, **AnyDesk** та **TeamViewer**, якщо вони не є частиною офіційного переліку ПЗ установи.
   - **Обґрунтування:** Проведення аудиту та блокування засобів віддаленого керування, які не входять до офіційного переліку ПЗ установи, безпосередньо відповідає вимогам заходу **PR.PS-05**. Згідно з методичними рекомендаціями, використання неавторизованого програмного забезпечення має бути заборонено, а платформи налаштовані на виконання лише схвалених суб'єктом продуктів. Також цей захід реалізує вимоги пункту **PR.PS-02** щодо видалення несанкціонованого ПЗ та сервісів, які становлять надмірні ризики для кібербезпеки. Це здійснюється на виконання Наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту».
2. **Заборона приховування розширень файлів (Налаштування GPO)**
   - **Пропозиція:** Через групові політики вимкнути функцію приховування розширень для відомих типів файлів.
   - **Шлях GPO:** `User Configuration -> Preferences -> Control Panel Settings -> Folder Options`.
   - **Дія:** Зняти позначку з пункту `Hide extensions for known file types`.
   - **Обґрунтування:** Це дозволить працівникам бачити справжню назву файлу (наприклад, `наказ.pdf.exe` замість `наказ.pdf`) і вчасно розпізнати загрозу. Захід сприяє виконанню вимог щодо захисту кінцевих точок відповідно до Наказу ДССЗІ № 75.
3. **Фільтрація вкладень із подвійним розширенням**
   - **Пропозиція:** Налаштувати поштові шлюзи на автоматичне блокування або карантин для вхідних листів, що містять файли з підозрілими комбінаціями розширень (`.pdf.exe`, `.docx.exe`, `.zip.exe`).
   - **Обґрунтування:** Превентивне блокування найбільш поширеного вектора доставки шкідливого ПЗ угрупованням UAC-0050, що корелюється з методичними рекомендаціями щодо захисту електронної пошти.

Додаткові матеріали

- Технічний аналіз атаки: UAC-0050 Targets Financial Institutions (The Hacker News)
- Рекомендації CERT-UA: Кіберзагрози з боку UAC-0050

Ринок цифрової зброї — Санкції проти російських брокерів «вразливостей нульового дня»

Суть загрози Міністерство фінансів США наклало санкції на російську компанію **Operation Zero** (Matrix LLC) та її власника за скуповування викрадених «експлойтів нульового дня» (zero-day). З'ясувалося, що вони придбали у колишнього співробітника американського оборонного підрядника 8 унікальних хакерських інструментів, розроблених виключно для уряду США. Ці інструменти дозволяють непомітно зламувати найпопулярніші операційні системи та месенджери.

Простими словами (Оцінка ризику) Уявіть, що зловмисники купили «універсальні відмички» до дверей, про існування яких виробник замків навіть не підозрює. Оскільки **Operation Zero** офіційно продає ці інструменти російським державним структурам, це означає, що спецслужби рф тепер мають на озброєнні професійні цифрові засоби для «невидимого» проникнення в будь-які системи на базі Windows, Android чи iOS. Для наших установ це означає, що традиційні антивіруси можуть не зафіксувати момент зламу, оскільки зловмисники використовують вразливості, на які ще немає «ліків» (патчів).

Рекомендовані напрями для опрацювання (Для IT-підрозділів / Підрозділів захисту інформації)

1. **Перехід на поведінковий аналіз загроз (EDR/XDR)**
   - **Пропозиція:** Розглянути можливість впровадження систем класу EDR (Endpoint Detection and Response), які фокусуються не на «підписах» вірусів, а на аномальній поведінці процесів.
   - **Обґрунтування:** Оскільки zero-day експлойти та складні цілеспрямовані атаки (APT) часто залишаються невидимими для традиційних засобів захисту, необхідне виявлення аномальної активності (наприклад, виконання коду легітимними програмами або несанкціоноване завантаження даних). Це безпосередньо відповідає вимогам заходів **DE.CM-01** (Моніторинг мереж, систем та фізичного середовища) та **DE.AE-02** (Аналіз виявлених аномалій для виявлення потенційних кіберінцидентів) відповідно до Наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту». Впровадження цих інструментів забезпечує проактивне виявлення загроз на ранніх етапах їх розповсюдження.
2. **Негайне встановлення критичних оновлень (Patch Management)**
   - **Пропозиція:** Налагодити процес встановлення оновлень безпеки протягом 24-48 годин після їх випуску вендорами (Microsoft, Google тощо).
   - **Обґрунтування:** Як тільки розробник випускає патч, «нульовий день» перестає бути секретною зброєю. Швидке оновлення систем у закладах є критично важливим для виконання вимог щодо захисту інформації та методичних рекомендацій відповідно до Наказу ДССЗІ № 75.
3. **Моніторинг новин про нові CVE (Vulnerability Intelligence)**
   - **Пропозиція:** Додати офіційні канали CERT-UA та вендорів ПЗ до щоденного моніторингу. У разі появи інформації про активну експлуатацію zero-day вразливостей у ПЗ, що використовується в установі — негайно вживати заходів з ізоляції таких систем.
   - **Обґрунтування:** Своєчасна поінформованість дозволяє фахівцям бути на крок попереду зловмисників, що корелюється з принципом **ID.RA-02 (Моніторинг джерел загроз)** відповідно до Наказу № 75.

Додаткові матеріали

- Офіційне повідомлення Мінфіну США: US Sanctions Russian Exploit Broker (Treasury.gov)
- Технічний контекст: Russian 'Operation Zero' Bounty for Zero-Days (BleepingComputer)

Системний захист — Блокування вразливих драйверів (Microsoft Driver Blocklist)

Суть технології Microsoft впровадила механізм **Vulnerable Driver Blocklist**, який забороняє запуск драйверів із відомими вразливостями. Це захищає систему від атак типу **BYOVD** (Bring Your Own Vulnerable Driver), коли зловмисник використовує легітимний, але «дірявий» драйвер для захоплення контролю над ядром системи. Захист актуальний для Windows 10/11 та Windows Server 2016–2025.

Простими словами (Оцінка ризику) Драйвер — це програма, яка має найвищий рівень доступу до «серця» комп'ютера (ядра системи). Зловмисники часто не зламують систему напряму, а підкидають їй старий, але легітимний драйвер відомого виробника, який має відому діру в безпеці. Через цю діру вони отримують повний контроль над пристроєм, обходячи навіть просунуті антивіруси. Функція Blocklist працює як «чорний список» на вході: навіть якщо драйвер виглядає справжнім, система не дасть йому запуститися, якщо він є у списку небезпечних.

Рекомендовані напрями для опрацювання (Для IT-підрозділів / Підрозділів захисту інформації)

1. **Централізоване керування через GPO (Технічний рецепт)**
   - **Пропозиція:** Примусово увімкнути захист на основі віртуалізації для всіх доменних комп'ютерів та серверів установи.
   - **Шлях GPO:** `Computer Configuration\Administrative Templates\System\Device Guard`
   - **Налаштування:** Увімкнути `Turn On Virtualization Based Security` та встановити параметр `Virtualization Based Protection of Code Integrity` у значення **Enabled with UEFI lock**. Це гарантує, що список блокування драйверів буде активним та захищеним від спроб вимкнення з боку шкідливого ПЗ.
2. **Активація цілісності пам'яті та відповідність Наказу № 75**
   - **Пропозиція:** Забезпечити контроль активації функцій «Цілісності пам'яті» (HVCI) та «Списку блокування вразливих драйверів» на всіх робочих станціях та серверах установи. На нових пристроях з Windows 11 перевірити коректність роботи цих функцій, а на застарілих системах та серверних платформах провести аудит сумісності драйверів для їх подальшого ввімкнення через групові політики (GPO) або додаток «Безпека Windows».
   - **Обґрунтування:** Використання засобів безпеки на основі віртуалізації та апаратного забезпечення безпосередньо відповідає вимогам пункту **PR.PS-06** (Встановлення та використання заходів безпеки, що базуються на апаратному забезпеченні) відповідно до Наказу Адміністрації Держспецзв'язку від 30.01.2026 № 75. Це дозволяє захистити критичні процеси ОС від впровадження шкідливого коду на рівні ядра (Kernel-mode) та нівелювати загрози типу BYOVD (Bring Your Own Vulnerable Driver), які часто використовуються під час складних кібератак на державний сектор.
3. **Моніторинг через журнал подій (Порада фахівця)**
   - **Пропозиція:** Щоб переконатися, що політика працює і не конфліктує з обладнанням, використовуйте **Event Viewer**.
   - **Шлях:** `Applications and Services Logs\Microsoft\Windows\CodeIntegrity\Operational`.
   - **Подія:** Шукайте **Event ID 3099** (успішне застосування політики). Якщо ви бачите **ID 3091**, це означає, що система заблокувала вразливий драйвер — у такому разі варто оновити драйвери відповідного пристрою до останньої версії від виробника.

Додаткові матеріали

- Технічне керівництво Microsoft: Recommended driver block rules

Інструментарій фахівця — Оновлення Parrot OS 7.1 для проведення аудитів безпеки

Суть оновлення Випущено оновлену версію Parrot OS 7.1 — спеціалізованої операційної системи на базі Debian, розробленої для тестування на вразливості, цифрової криміналістики та гарантування приватності. Основною новацією є інтеграція інструменту **MCPwn**, який дозволяє використовувати мовні моделі (LLM, як-от Gemini або Claude) для автоматизації роботи засобів сканування мережі (nmap, sqlmap тощо) у у захищеному середовищі.

Простими словами (Оцінка можливостей) Для того, щоб ефективно захищати внутрішні системи (файлові сервера, внутрішні сервіси, поштові сервери), фахівцям IT-підрозділів/Підрозділів захисту інформації пкорисно володіти інструментами, які дозволяють подивитися на власну мережу. Parrot OS 7.1 — це «цифрова лабораторія», де вже зібрані всі необхідні інструменти для виявлення слабких місць та пошуку вразливостей. Використання таких рішень у тестовому режимі дозволяє виявити критичні недоліки налаштувань (наприклад, відкриті порти чи застарілі версії служб) до того, як їх виявить зловмисник.

Рекомендовані напрями для опрацювання (Action Items для керівників та IT-підрозділів/Підрозділів захисту інформації)

1. **Оцінка доцільності розгортання тестового середовища**
   - **Пропозиція:** Розглянути можливість використання Parrot OS 7.1 як платформи для проведення періодичних внутрішніх аудитів безпеки.
   - **Контекст:** Рекомендується проводити такі перевірки на окремих робочих станціях або в ізольованих віртуальних машинах, щоб забезпечити безпеку самого процесу аналізу та уникнути впливу на робочі процеси установи.
2. **Апробація інструментів автоматизації (MCPwn)**
   - **Пропозиція:** Протестувати функціональність інструменту MCPwn для автоматизованого збору інформації про стан мережевого обладнання.
   - **Контекст:** Важливо врахувати архітектурну особливість інструменту — ізоляцію команд у Docker-контейнерах, що є безпечним методом використання ШІ-асистентів для технічного моніторингу.
3. **Використання як бази для фахового розвитку**
   - **Пропозиція:** Розглянути вбудований інструментарій системи як основу для підвищення практичних навичок фахівців у сфері кіберзахисту.
   - **Контекст:** Ознайомлення з методами симуляції атак підвищує загальну готовність підрозділів до реагування на реальні інциденти.

Додаткові матеріали

- Офіційні відомості про реліз: Parrot OS 7.1 Release Notes
- Спільнота та документація: ParrotOS Documentation Community