

# Кібер-дайджест МОЗ України

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



## Нові правила аудиту — Держспецзв'язку затвердило єдину методику оцінювання кіберзахисту (Наказ № 285)



**Суть оновлення** Держспецзв'язку Наказом № 285 (від 16.04.2026) затвердило комплекс методичних рекомендацій для оцінювання стану кіберзахисту. Відтепер аудит перетворюється на процедуру з чітким математичним апаратом. Стан безпеки розраховується за 6 базовими функціями (управління, ідентифікація, захист, виявлення, реагування, відновлення) та вимірюється за 5-рівневою шкалою зрілості. Окремо затверджено єдину уніфіковану форму звіту для всіх суб'єктів забезпечення кібербезпеки.



**Простими словами (Оцінка ризику)** До прийняття цього наказу оцінка стану безпеки могла мати елементи суб'єктивності. Тепер держава впроваджує жорсткий «принцип критичної ланки». Що це означає на практиці: якщо хоча б одна з базових функцій в установі (наприклад, реагування на інциденти) оцінена нижче ніж у 20%, загальний стан безпеки автоматично визнається «критичним». Більше неможливо приховати серйозні прогалини чи вразливості за рахунок загальних високих балів з інших напрямів. Також нова шкала зрілості фокусується не лише на наявності обладнання чи програмного забезпечення, а й на тому, наскільки якісно процеси задокументовані та інтегровані в щоденну роботу персоналу установи.



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

- Практичний крок: Тестове самооцінювання за новими правилами**
  - Пропозиція:** Визначити реальний стан кіберзахисту установи до офіційних перевірок.
  - Дія:** Підрозділам захисту інформації **доцільно** ознайомитися з новою методологією та уніфікованою формою звіту, щоб провести внутрішнє пілотне самооцінювання. Це дозволить побачити свій рівень зрілості через призму нових вимог регулятора та виявити найбільш слабкі місця («критичні ланки»).
- Відповідність нормативним вимогам (Документування процесів)**
  - Пункт:** Підтвердження рівня зрілості (від 0 до 4) згідно з Наказом № 285.
  - Обґрунтування:** Згідно з новими правилами, навіть якщо система фізично захищена, але ці заходи не описані в політиках чи інструкціях (СОПах), установка не зможе отримати високий рівень зрілості. **Рекомендується** провести ревізію внутрішньої документації з IT-безпеки, щоб вона відповідала реальним процесам у закладі.
- Фокус на пріоритетних функціях (Стратегічне планування)**
  - Пропозиція:** Рационально розподілити ресурси на захист інфраструктури.
  - Дія:** Згідно з методикою Держспецзв'язку, найбільшу вагу при розрахунку мають функції «захист» та «виявлення». Тому під час планування IT-бюджетів чи модернізації інфраструктури **варто** приділяти першочергову увагу саме системам активного моніторингу та захисту мережі.



### Додаткові матеріали

- Офіційне повідомлення: [Держспецзв'язку впроваджує єдині підходи до оцінювання стану кіберзахисту \(Держспецзв'язку\)](#)

## Атака UAC-0244 — Кібершпигунство під виглядом гуманітарної допомоги



**Суть оновлення** Протягом березня – квітня 2026 року CERT-UA зафіксував різке зростання інтенсивності атак угруповання **UAC-0244** (раніше відомого як UAC-0247), спрямованих на органи місцевого самоврядування та заклади охорони здоров'я. Зловмисники застосовують тактику соціальної інженерії: надсилають електронні листи щодо «надання гуманітарної допомоги» з посиланням на завантаження архіву з нібито формами для заповнення. Запуск файлу з архіву призводить до ураження пристроїв шкідливим ПЗ: **AGINGFLY** (дистанційне керування), **CHROMELEVATOR** (викрадення паролів з браузерів) та **ZAPIXDESK** (викрадення даних WhatsApp). Окремий вектор атаки націлений на Сили оборони через месенджер Signal під виглядом оновлення ПЗ «BACHU».



**Простими словами (Оцінка ризику)** Ця атака — не просто технічна загроза, а спроба встановити повний негласний контроль над робочими станціями спеціалістів. Оскільки хакери викрадають автентифікаційні дані (паролі) та доступ до месенджерів, під прямим ударом опиняється конфіденційність листування та доступ до державних реєстрів. Використання легенди про «гуманітарну допомогу» — це цинічна експлуатація довіри в умовах війни. Головний ризик для установи — тривалий простій систем через компрометацію мережі та потенційний шантаж витоком медичних чи службових даних.



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

- Практичний крок:**
  - Підрозділам захисту інформації доцільно обмежити запуск LNK-, HTA- та JS-файлів, а також використання штатних утиліт *mshta.exe*, *powershell.exe* та *wscript.exe* для користувачів, чиї службові обов'язки не потребують роботи з цими інструментами.
- Відповідність нормативним вимогам**
  - Реалізація цих обмежень відповідає вимогам **Наказу ДССЗІ № 75** щодо скорочення поверхні атаки та застосування штатних механізмів захисту операційної системи.
- Стратегічне планування**
  - Керівникам рекомендуємо ініціювати позаплановий інструктаж персоналу щодо ризиків соціальної інженерії, наголосивши: будь-які посилання на «форми» у листах про допомогу мають перевірятися IT-підрозділом до моменту відкриття.



### Додаткові матеріали

- CERT-UA: Лікарні та органи місцевого самоврядування у фокусі UAC-0244 — <https://cert.gov.ua/article/6288271>

## Компрометація робочих місць — 108 шкідливих розширень Chrome викрадають дані Google та Telegram



**Суть оновлення** Дослідники виявили масштабну кіберкампанію, під час якої 108 шкідливих розширень для браузера Google Chrome збирають дані понад 20 000 користувачів. Маскуючись під клієнти Telegram, ігри, перекладачі та утиліти, ці додатки викрадають токени авторизації Google (OAuth2), перехоплюють сесії Telegram Web та вбудовують бекдори для виконання шкідливого коду. У вихідному коді розширень виявлено російськомовні коментарі, а всі викрадені дані передаються на єдиний ворожий сервер (IP 144.126.135[.]238).



**Простими словами (Оцінка ризику)** Працівники закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ), прагнучи оптимізувати роботу, іноді вдаються до самовільного встановлення неофіційних "помічників" для браузера в обхід корпоративних політик безпеки. Це створює неконтрольований канал витоку службової інформації. Через такі сторонні додатки зловмисники можуть непомітно отримувати доступ до корпоративного листування, файлів на дисках та робочих чатів. Цей витік облікових даних є прямим шляхом до масштабної компрометації внутрішньої мережі установи, що створює критичний ризик блокування інформаційних систем та тривалого простою в наданні послуг.



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

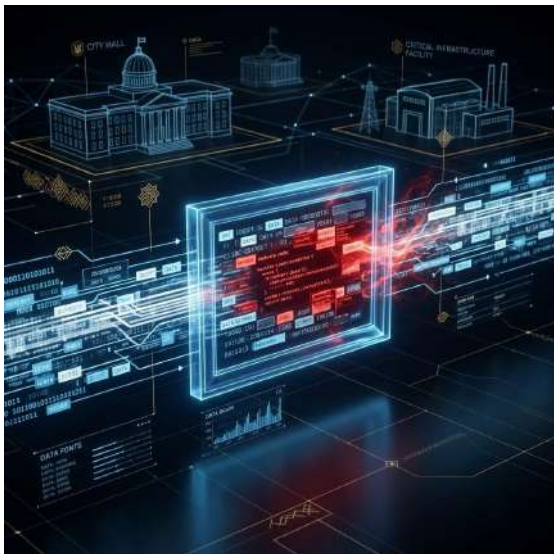
- Практичний крок:**
  - Підрозділам захисту інформації та кіберзахисту доцільно оперативно заблокувати на рівні корпоративного міжмережевого екрана IP-адресу командного сервера (144.126.135[.]238) та перевірити мережу на наявність інших індикаторів компрометації (IoC). Також рекомендуємо провести цільовий інструктаж персоналу щодо небезпеки сторонніх додатків та ініціювати примусове завершення активних сесій Telegram Web на робочих станціях.
- Відповідність нормативним вимогам**
  - Контроль за встановленням ПЗ відповідає вимогам Наказу ДССЗІ № 75, зокрема пункту PR.PT-01 (Управління конфігураціями). Управління дозволенням програмним забезпеченням є обов'язковим базовим заходом у рамках формування цільового профілю безпеки для успішного проходження Авторизації систем (згідно з Постановою КМУ № 712).
- Стратегічне планування**
  - Для системного вирішення проблеми ІТ-підрозділам варто запровадити керування браузерами через групові політики безпеки (GPO). Доцільно налаштувати стратегію «білих списків»: технічно заборонити користувачам встановлення будь-яких зовнішніх розширень, крім тих, що пройшли перевірку та офіційно затверджені для службових потреб.



### Додаткові матеріали

- Повний список шкідливих розширень та індикатори компрометації (IoC) — <https://socket.dev/blog/108-chrome-ext-linked-to-data-exfil-session-theft-shared-c2>
- Огляд зарози: 108 Malicious Chrome Extensions Steal Google and Telegram Data — <https://thehackernews.com/2026/04/108-malicious-chrome-extensions-steal.html>

## Шпигунство та деструктивні дії — Російське угруповання APT28 атакує держустанови новим комплексом PRISMEX



**Суть оновлення** Дослідники Trend Micro виявили масштабну кіберкампанію російського угруповання APT28 (Pawp Storm), спрямовану проти державних установ України та логістичних партнерів НАТО. Зловмисники застосовують раніше невідомий комплекс шкідливого ПЗ під назвою PRISMEX. Атака поєднує експлуатацію вразливостей нульового дня в ОС Windows (CVE-2026-21509 та CVE-2026-21513) та техніку стеганографії — приховування шкідливого коду всередині звичайних зображень (.png). Вірус використовує легітимні хмарні сервіси для управління, викрадає корпоративне листування з Outlook, а також містить деструктивний модуль (Wiper), здатний безповоротно видаляти всі файли з комп'ютерів.



**Простими словами (Оцінка ризику)** Хакери суттєво ускладнили методи атак: вони ховають віруси не в підозрілих файлах, а у звичайних картинках, які стандартні антивіруси пропускають як безпечні. Для зв'язку зі своїм сервером вірус маскує трафік під роботу хмарних сховищ, що робить його "невидимим" для корпоративних міжмережєвих екранів. Ця загроза несе подвійний ризик для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ): по-перше, ворог отримує негласний доступ до службової документації та пошти; по-друге, хакери можуть віддалено запустити команду на фізичне знищення даних. Це загрожуватиме повною зупинкою операційних процесів установи через втрату доступу до інформаційно-комунікаційних систем (ІКС).



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

- Практичний крок:**
  - Підрозділам захисту інформації та кіберзахисту доцільно налаштувати поштові шлюзи на жорстке блокування або карантин вкладень із файлами ярликів (.LNK). Критично важливо переконатися, що на всіх робочих станціях та серверах розгорнуто останні оновлення безпеки Microsoft (Patch Management), які закривають згадані вразливості системи.
- Відповідність нормативним вимогам**
  - Оперативне усунення вразливостей (ID.RA-01) та контроль за виконанням коду (PR.PT-02) є обов'язковими базовими заходами кіберзахисту згідно з Наказом ДССЗІ № 75. Системний підхід до оновлення інфраструктури — це невіддільна частина системи управління ризиками (RMF) та підтримки цільового профілю безпеки установи.
- Стратегічне планування**
  - Оскільки фінальною стадією атаки є запуск модуля Wiper (знищення даних), керівникам доцільно доручити ІТ-підрозділам проведення позапланової перевірки стану виконання стандартних операційних процедур (СОП) щодо резервного копіювання. Наявність ізольованих (офлайн) або незмінних (immutable) резервних копій ключових інформаційних систем (ІС) та баз даних — це надійний інструмент забезпечення безперервності роботи установи у випадку деструктивної кібератаки.



**Додаткові матеріали**

- The Hacker News: APT28 Deploys PRISMEX Malware in Campaign Targeting Ukraine and NATO Allies — <https://thehackemews.com/2026/04/apt28-deploys-prismex-malware-in.html>

## Компрометація мережевого обладнання — Угруповання APT28 перехоплює DNS-трафік через маршрутизатори TP-Link та MikroTik



**Суть оновлення** Російське кіберугруповання APT28 (Forest Blizzard) проводить масштабну кампанію з компрометації SOHO-маршрутизаторів (зокрема TP-Link та MikroTik). Зловмисники використовують вразливості (наприклад, CVE-2023-50224) для несанкціонованої зміни налаштувань DNS на пристроях. Це дозволяє непомітно перенаправляти локальний мережевий трафік на підконтрольні хакерам вузли для проведення атак типу Attacker-in-the-Middle (AiTM). Основна мета — пасивний збір даних та викрадення облікових даних, паролів і токенів OAuth без жодної взаємодії з користувачем. Кампанія орієнтована на державні установи, військових та об'єкти критичної інфраструктури, при цьому зафіксовано цілеспрямовані дії проти пристроїв MikroTik безпосередньо в Україні.



**Простими словами (Оцінка ризику)** Уявіть, що працівник вводить правильну адресу корпоративної пошти чи інформаційно-комунікаційної системи (ІКС), але скомпрометований маршрутизатор непомітно перенаправляє його на точну хакерську копію цього ресурсу. Працівник вводить пароль, і він миттєво опиняється у ворога. Оскільки злам відбувається на рівні базового мережевого обладнання, стандартні антивіруси на комп'ютерах можуть не помітити підміни трафіку. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) це створює прямий ризик компрометації облікових записів адміністраторів та персоналу. Наслідки — несанкціонований доступ до внутрішніх систем та можливий тривалий простій закладу через втрату контролю над мережею.



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

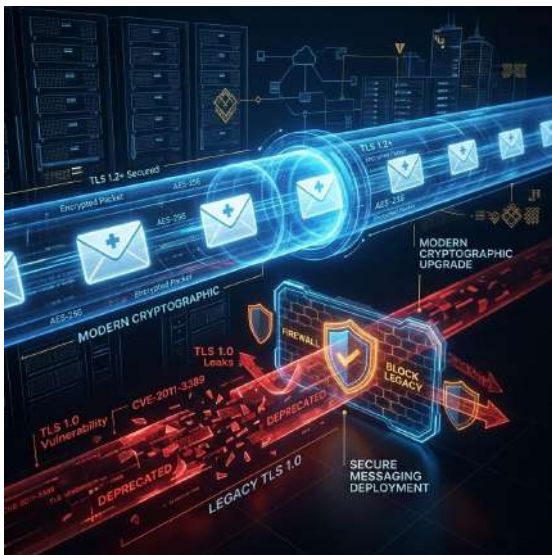
- Практичний крок:**
  - Підрозділам захисту інформації доцільно провести позапланову інвентаризацію периферійного мережевого обладнання та SOHO-маршрутизаторів. Варто перевірити конфігурації DNS-серверів на цих пристроях на предмет несанкціонованих змін та оновити прошивки до актуальних версій, щоб закрити вразливості доступу (зокрема CVE-2023-50224).
- Відповідність нормативним вимогам**
  - Контроль за конфігураціями мережевого обладнання та управління вразливостями прямо відповідають вимогам Наказу ДССЗІ № 75 (базові заходи PR.PT-01 та ID.RA-01). Систематичне оновлення мікропрограм та моніторинг DNS-трафіку (DE.CM-01) є обов'язковими компонентами для підтримання цільового профілю безпеки установи та дотримання принципів системи управління ризиками (RMF) згідно з Постановою КМУ № 712.
- Стратегічне планування**
  - Керівникам доцільно підтримати ініціативи IT-підрозділів щодо поступової відмови від використання побутових маршрутизаторів (SOHO) у корпоративному контурі на користь рішень корпоративного класу. Також рекомендуємо налаштувати на рівні головного міжмережевого екрана заборону на прямі зовнішні DNS-запити від звичайних пристроїв, примусово спрямовуючи трафік виключно через перевірені корпоративні DNS-сервери.



**Додаткові матеріали**

- The Hacker News: Russian State-Linked APT28 Exploits SOHO Routers in Global DNS Hijacking Campaign <https://thehackernews.com/2026/04/russian-state-linked-apt28-exploits.html>

## Інфраструктурні зміни — Microsoft повністю блокує застарілі протоколи TLS 1.0/1.1 в Exchange Online



**Суть оновлення** Починаючи з липня 2026 року, Microsoft остаточно припиняє підтримку та блокуватиме з'єднання через застарілі криптографічні протоколи TLS 1.0 та TLS 1.1 для поштових клієнтів, що використовують POP3 та IMAP4 в Exchange Online. Раніше використання цих протоколів було можливе за умови явного налаштування для окремих вузлів, проте тепер підтримка скасовується повністю на користь сучасних стандартів TLS 1.2 та вище. Усі пристрої, скрипти або програми, які спробують підключитися до сервісу через старі протоколи, отримуватимуть відмову в доступі.



**Простими словами (Оцінка ризику)** Хоча більшість сучасних поштових програм на комп'ютерах працівників уже давно використовують нові стандарти шифрування, ризик криється в невидимій інфраструктурі. У закладах охорони здоров'я та на об'єктах критичної інфраструктури (ОКІ) може працювати спеціалізоване медичне обладнання, мережеві сканери, МФП, системи оповіщення або застарілі самописні інформаційно-комунікаційні системи (ІКС), які автоматично відправляють звіти чи результати на пошту через базові протоколи POP/IMAP. Якщо такі пристрої використовують старі стандарти TLS, з липня вони просто втратять здатність відправляти та отримувати електронні листи. Це може призвести до зупинки автоматизованих процесів обміну даними та збоїв у внутрішньому документообігу установи.



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

- Практичний крок:**
  - IT-підрозділам доцільно оперативно провести аудит поштових налаштувань. Варто перевірити не лише робочі станції, але й усе периферійне та спеціалізоване обладнання, яке інтегроване з корпоративною поштою. Необхідно переконатися, що системи налашовані на роботу з TLS 1.2 або вище. За потреби варто звернутися до вендорів обладнання для отримання оновлень мікропрограм (прошивок).
- Відповідність нормативним вимогам**
  - Відмова від використання застарілих та скомпрометованих криптографічних протоколів відповідає вимогам Наказу ДССЗІ № 75 щодо захисту даних під час їх передачі (PR.DS-02) та управління конфігураціями (PR.PT-01). Дотримання сучасних стандартів криптографії є обов'язковим елементом системи управління ризиками (RMF) та важливою умовою для успішного проходження Авторизації систем.
- Стратегічне планування**
  - IT-підрозділам доцільно розробити план поступової відмови від використання застарілих протоколів автентифікації (POP3/IMAP4) у корпоративній мережі та переходу на захищені сучасні API-з'єднання (наприклад, Microsoft Graph API). Керівникам установ рекомендується погодити цей план та забезпечити адміністративну підтримку процесу модернізації.



**Додаткові матеріали**

- BleepingComputer: Microsoft to deprecate legacy TLS in Exchange Online starting July — <https://www.bleepingcomputer.com/news/microsoft/microsoft-to-deprecate-legacy-tls-in-exchange-online-starting-july/>

## Атаки на ланцюг постачання — Ransomware-інцидент у провайдера медичних ІКС ChipSoft



**Суть оновлення** Нідерландський розробник медичного програмного забезпечення ChipSoft, який постачає системи електронних медичних карток (EHR), зазнав кібератаки із застосуванням вірусу-вимагача (Ransomware). Інцидент змусив компанію відключити свої цифрові послуги, зокрема вебпортали та мобільні додатки. Як наслідок, низка закладів охорони здоров'я в Нідерландах та Бельгії, що використовують платформу HiX, зіткнулися з перебоями в роботі. Провайдер офіційно рекомендував установам превентивно відключитися від своїх систем на час проведення розслідування та очищення інфраструктури.



**Простими словами (Оцінка ризику)** Цей інцидент яскраво ілюструє загрозу атак на ланцюг постачання (Supply Chain Attack). Зловмисникам не обов'язково проникати в мережу кожного закладу окремо — достатньо скомпрометувати центрального провайдера ІТ-послуг. Для об'єктів критичної інфраструктури (ОКІ) це означає ризик миттєвого блокування доступу до централізованих інформаційно-комунікаційних систем (ІКС) через зовнішній фактор. Крім того, атаки вірусів-вимагачів сьогодні мають подвійний вектор: вони не лише шифрують файли для створення простою, але й викрадають бази даних, що створює серйозний ризик шантажу оприлюдненням чутливої інформації.



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

- Практичний крок:**
  - ІТ-підрозділам та Підрозділам захисту інформації доцільно провести ревізію зовнішніх підключень. Рекомендуємо переконатися, що доступ сторонніх сервісів та розробників до внутрішньої мережі установи жорстко сегментований. Варто перевірити, що всі підрядники, які здійснюють віддалену технічну підтримку медичного обладнання чи ІКС, використовують виключно багатофакторну автентифікацію (MFA) для доступу.
- Відповідність нормативним вимогам**
  - Контроль за постачальниками послуг прямо відповідає вимогам Наказу ДССЗІ № 75 (функція "Управління", категорія "Управління ризиками ланцюга постачання" — GV.SC). Також, в рамках впровадження системи управління ризиками (RMF) за Постановою КМУ № 712, для ефективного захисту від програм-вимагачів заклади повинні мати не лише ізольовані (офлайн) бекапи (для швидкого відновлення працездатності), але й застосовувати шифрування баз даних (щоб унеможливити шантаж у разі витоку).
- Стратегічне планування**
  - Керівникам доцільно ініціювати розробку або актуалізацію Стандартних операційних процедур (СОП) щодо забезпечення безперервності діяльності (Business Continuity). Кожен заклад охорони здоров'я повинен мати чіткий алгоритм автономної роботи, якщо виникне необхідність екстрено розірвати зв'язок із центральними провайдерами для локалізації кіберзагрози.

**Додаткові матеріали**



- BleepingComputer: Healthcare IT solutions provider ChipSoft hit by ransomware attack — <https://www.bleepingcomputer.com/news/security/healthcare-it-solutions-provider-chipsoft-hit-by-ransomware-attack/>

## Стратегія захисту — Штучний інтелект змінює парадигму кібербезпеки: від статичних аудитів до моніторингу в реальному часі



**Суть оновлення** Експерти з кібербезпеки наголошують на необхідності докорінної зміни підходів до управління ризиками в епоху штучного інтелекту. Новітні ШІ-моделі (наприклад, Claude Mythos) здатні аналізувати та експлуатувати вразливості за лічені хвилини без втручання людини. Це нівелює ефективність класичних статичних перевірок: кварталні аудити та періодичні пентести відображають лише стан безпеки в минулому, а не поточну реальність. Фокус уваги IT-керівників має зміститися на безперервний моніторинг інфраструктури (runtime visibility), управління людськими та машинними ідентифікаторами, а також на застосування систем ШІ як допоміжного інструменту аналітики. Такі технології мають допомагати фахівцям швидше опрацьовувати великі масиви даних про інциденти, залишаючи при цьому прийняття остаточних рішень та контроль виключно за людиною.



**Простими словами (Оцінка ризику)** Успішно пройдений аудит показує, наскільки захищеною система була вчора, але не гарантує безпеки сьогодні. Зловмисники більше не витрачають тиждень на пошук слабких місць — ШІ робить це миттєво. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) це означає, що ризик зміщується у бік невидимих загроз. Неконтрольовані "машинні" облікові записи або надмірні права доступу можуть бути скомпрометовані за хвилини, що призведе до повної зупинки інформаційно-комунікаційних систем (ІКС) ще до того, як адміністратор отримає перше сповіщення. Спроможність бачити загрозу та реагувати на неї в режимі реального часу стає ключовою умовою забезпечення безперервності роботи установи.



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

- Практичний крок:**
  - Підрозділам захисту інформації доцільно провести повну інвентаризацію всіх облікових записів (включно з підрядниками, сервісними акаунтами та API-ключами). На основі цього слід впровадити принцип найменших привілеїв, прибравши надмірні права доступу. Також варто перевірити налаштування систем моніторингу для забезпечення видимості подій в інфраструктурі "тут і зараз".
- Відповідність нормативним вимогам**
  - Перехід від статичного "паперового" комплаєнсу до безперервного управління ризиками є фундаментальною основою фреймворку RMF згідно з Постановою КМУ № 712. Інвентаризація облікових записів та управління доступом є обов'язковими базовими заходами відповідно до Наказу ДССЗІ № 75 (пункти PR.AC-01 та PR.AC-04 щодо контролю ідентифікаторів).
- Стратегічне планування**
  - IT-підрозділам рекомендується розробити та актуалізувати Стандарти операційні процедури (СОП) щодо реагування на швидкі кіберінциденти. Керівникам установ доцільно погодити ці СОПи та ініціювати регулярні спільні кібернавчання (настільні симуляції) для відпрацювання алгоритму дій команди: від виявлення загрози до кризової комунікації та відновлення роботи систем.



**Додаткові матеріали**

- CyberScoop: The AI era demands a different kind of CISO — <https://cyberscoop.com/ciso-strategy-ai-real-time-risk-op-ed/>

## Регіональні загрози — Масштабна кібератака на медичну систему Республіки Молдова



**Суть оновлення** У Республіці Молдова зафіксовано масштабну кібератаку на медичну базу даних. Інцидент призвів до компрометації близько 30% масиву даних, який містив персональну інформацію пацієнтів та дані щодо платежів у системі охорони здоров'я. За даними Агентства з кібербезпеки Молдови, зловмисники не висували вимог щодо викупу. Фахівці не виключають, що це цілеспрямована операція спецслужб російської федерації з метою викрадення чутливої інформації.



**Простими словами (Оцінка ризику)** Цей інцидент у сусідній країні є дуже чітким сигналом для вітчизняних закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ). Відсутність фінансових вимог з боку хакерів свідчить про те, що ворог зосереджений на шпигунстві та зборі розвідувальних даних, а не на швидкому збагаченні. Успішна атака такого типу на наші інформаційно-комунікаційні системи (ІКС) може призвести до масштабного витоку медичних даних громадян та серйозного порушення безперервності роботи установ. Окрім прямої шкоди операційним процесам, такі витоки створюють величезні репутаційні ризики та можуть бути використані ворогом для інформаційно-психологічних операцій (ІПСО).

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



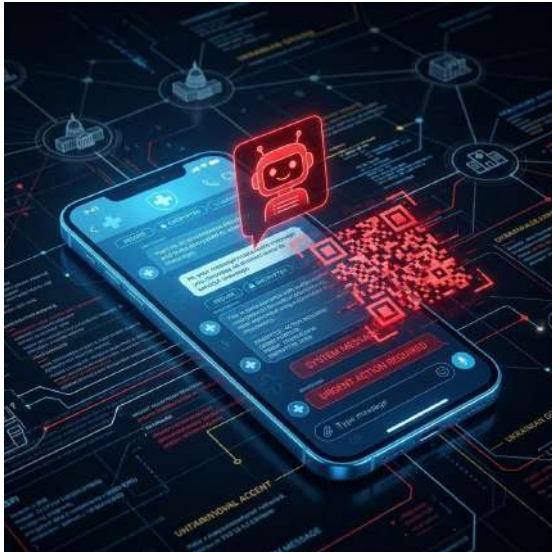
- Практичний крок:**
  - Підрозділам захисту інформації та кіберзахисту доцільно провести перевірку систем моніторингу мережевого трафіку на наявність аномальної активності, що може свідчити про несанкціоноване вивантаження великих обсягів даних (Data Exfiltration). Також рекомендується вкотре переконатися в актуальності та ізольованості існуючих резервних копій (бекапів) критичних баз даних.
- Відповідність нормативним вимогам**
  - Захист баз даних та запобігання витокам інформації є ключовим елементом вимог Наказу ДССЗІ № 75 (зокрема, функція «Забезпечення захисту», категорія «Безпека даних» — PR.DS). Застосування механізмів шифрування чутливих даних (як у стані спокою, так і під час передачі) є необхідною складовою впровадження системи управління ризиками (RMF) згідно з Постановою КМУ № 712.
- Стратегічне планування**
  - ІТ-підрозділам рекомендується розробити або актуалізувати Стандарти операційні процедури (СОП) щодо алгоритму дій у разі виявлення спроб несанкціонованого доступу до ІКС. Керівникам установ доцільно забезпечити адміністративну підтримку процесу модернізації систем захисту, зокрема розглянути можливість поступового впровадження рішень класу DLP (Data Loss Prevention) для контролю за рухом конфіденційної інформації та мінімізації ризиків масового витоку.



### Додаткові матеріали

- TVR Moldova: "30% din date afectate". Sistemul medical al R. Moldova a fost supus unui atac cibernetice masiv — <https://tvr Moldova.md/article/38e53cd804217aa4/30-din-date-afectate-sistemul-medical-al-r-moldova-a-fost-supus-unui-atac-cibernetice-masiv.html>

## Соціальна інженерія — Російські хакери зламують акаунти Signal високопосадовців через фейкових ботів



**Суть оновлення** Урядові структури Німеччини та Нідерландів фіксують масштабну фішингову кампанію, спрямовану на користувачів месенджера Signal (посадовців, військових, журналістів). За атаками, ймовірно, стоять підконтрольні РФ кібергрупування. Механіка зламу не передбачає злому криптографії: зловмисники створюють фейкового чат-бота «Служби безпеки Signal», який повідомляє жертві про нібито підозрілу активність. Для «захисту» акаунта бот вимагає терміново ввести PIN-код або відсканувати QR-код. Виконання цих дій дозволяє хакерам непомітно прив'язати обліковий запис до свого пристрою, отримуючи повний доступ до контактів та історії листування.



**Простими словами (Оцінка ризику)** Ворог успішно використовує базу психологію — створює відчуття терміновості та страху втрати даних. Якщо співробітник закладу охорони здоров'я або об'єкта критичної інфраструктури (ОКІ) піддається на цю маніпуляцію, зловмисники отримують негласний доступ до його смартфона. Це створює критичний ризик витоку службової інформації, планів реагування та контактних баз. Більше того, скомпрометований акаунт керівника може бути використаний для розсилки шкідливого ПЗ колегам або проведення інформаційно-психологічних операцій (ІПСО) всередині установи, що прямо загрожує безперервності операційних процесів.



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

- 1. Практичний крок:**
  - Підрозділам захисту інформації та кіберзахисту доцільно провести оперативний цільовий інструктаж персоналу. Необхідно наголосити: офіційна підтримка месенджерів ніколи не звертається до користувачів у чатах із вимогою надати PIN-код чи відсканувати QR-код. Також варто зобов'язати працівників перевірити розділ «Пов'язані пристрої» (Linked Devices) та активувати функцію «Блокування реєстрації» (Registration Lock) у налаштуваннях конфіденційності.
- 2. Відповідність нормативним вимогам**
  - Систематичне підвищення обізнаності персоналу щодо ризиків соціальної інженерії (PR.AT-01) є обов'язковим базовим заходом кіберзахисту згідно з Наказом ДССЗІ № 75. Навчання співробітників основам кібергігієни є невіддільною частиною загальної системи управління ризиками (RMF) та підтримки цільового профілю безпеки відповідно до Постанови КМУ № 712.
- 3. Стратегічне планування**
  - IT-підрозділам рекомендується розробити Стандарти операційні процедури (СОП) щодо використання публічних месенджерів для службової комунікації. Керівникам установ доцільно затвердити ці регламенти та забезпечити організаційну підтримку поступового переходу команд на використання виключно корпоративних, контрольованих каналів зв'язку для обміну чутливою робочою інформацією.



### Додаткові матеріали

- SecurityWeek: Germany Suspects Russia Is Behind Signal Phishing That Targeted Top Officials — <https://www.securityweek.com/germany-suspects-russia-is-behind-signal-phishing-that-targeted-top-officials/>

## Інновації у розробці — IBM випускає ШІ-помічника Bob для автоматизації повного циклу розробки (SDLC)



**Суть оновлення** Компанія IBM офіційно презентувала Bob — спеціалізованого ШІ-асистента для корпоративних команд розробників. На відміну від звичайних генераторів коду, Bob інтегрується в увесь життєвий цикл створення ПЗ (SDLC): від планування та кодування до тестування, розгортання та модернізації старих систем. Система використовує підхід "multi-model orchestration" (динамічний вибір оптимальної ШІ-моделі під конкретну задачу: Claude, Mistral або власні моделі IBM Granite) для забезпечення точності та контролю витрат. Головна особливість Bob — збудовані з першого дня механізми безпеки, комплаєнсу та аудиту: сканування на наявність чутливих даних, перевірка політик у реальному часі та фіксація кожного кроку розробки (Auditability).



**Простими словами (Оцінка ризику)** Сучасні ШІ-помічники для кодування допомагають писати код дуже швидко, але часто цей "швидкий" код містить приховані вразливості, архітектурні помилки або порушує корпоративні стандарти безпеки. Як зазначають розробники, швидкий ШІ без належного контролю — це "просто швидкий ризик". Інструмент від IBM вирішує цю проблему: він не просто генерує рядки коду, а діє як віртуальний інженер з безпеки (Security Engineer) безпосередньо під час написання програми. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ), які розробляють власні інформаційно-комунікаційні системи (ІКС) або інтегрують сторонні рішення, доцільно розглянути використання подібних "керованих" ШІ-інструментів. Такий підхід може стати надійним запобіжником, що дозволить мінімізувати ризики потраплення неперевіреного коду з вразливостями у робоче середовище (Production).



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

- Практичний крок:**
  - IT-підрозділам та підрозділам розробки (якщо такі є в установі) доцільно переглянути поточний інструментарій використання ШІ. Варто заборонити розробникам використовувати публічні неконтрольовані ШІ-чати (наприклад, звичайний ChatGPT) для генерації або перевірки службового коду, оскільки це створює ризик витоку інтелектуальної власності та впровадження вразливостей. Натомість рекомендується розглянути перехід на спеціалізовані Enterprise-рішення з функціями аудиту (як-от IBM Bob, GitHub Copilot Enterprise тощо).
- Відповідність нормативним вимогам**
  - Забезпечення безпеки на етапі розробки та модернізації ПЗ прямо відповідає вимогам Наказу ДССЗІ № 75, зокрема заходам щодо безпечної розробки (PR.PS-03: Управління життєвим циклом розробки програмного забезпечення). Використання інструментів з вбудованим скануванням та аудитом дій розробників допомагає виконати ці вимоги та є вагомим плюсом при проходженні Авторизації системи згідно з Постановою КМУ № 712.
- Стратегічне планування**
  - Керівникам доцільно ініціювати оновлення внутрішніх регламентів (СОПів) щодо процесу розробки та модернізації ІКС. Незалежно від того, які ШІ-інструменти використовуються, фінальне слово завжди має залишатися за людиною. Рекомендується впровадити правило: будь-який згенерований або змінений за допомогою ШІ код (навіть "безпечним" асистентом) підлягає обов'язковому мануальному огляду (Code Review) та тестуванню на безпеку перед впровадженням.



**Додаткові матеріали**

- IBM Newsroom: Introducing IBM Bob: AI Development Partner — <https://newsroom.ibm.com/2026-04-28-introducing-ibm-bob-ai-development-partner-that-takes-enterprises-from-ai-assisted-coding-to-production-ready-software>