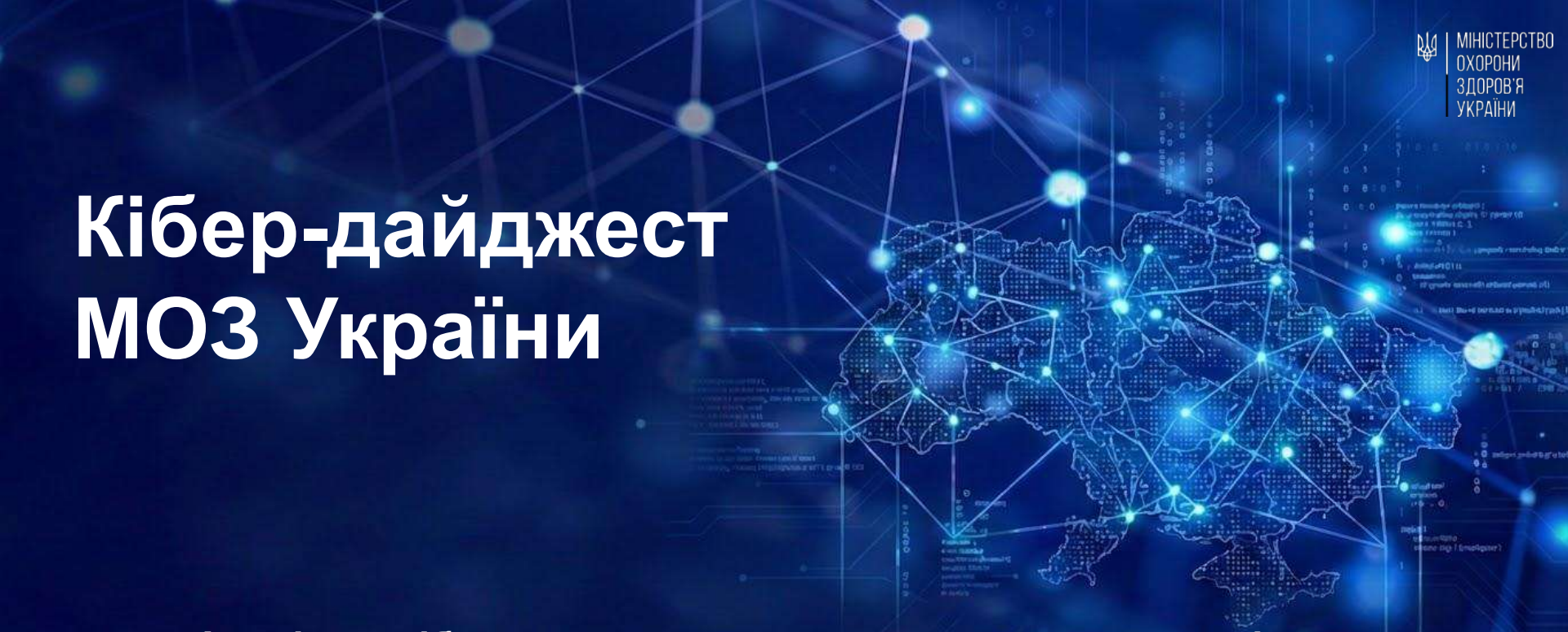
МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

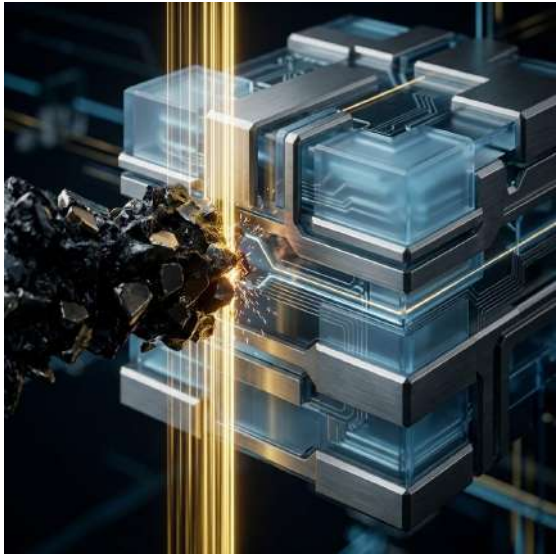
Кібер-дайджест МОЗ України



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

Червень 2026

Нормативні оновлення — Розширення переліку забороненого ПЗ та комунікаційного обладнання до 880 позицій



Суть оновлення Протягом червня 2026 року Адміністрація Держспецзв'язку провела два масштабних оновлення Переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання, розширивши його з 40 до 880 позицій. Оновлення базується на рішеннях РНБО щодо підсанкційних виробників. До списку додано антивіруси (Dr. Web, Kaspersky Lab), популярні бухгалтерські та ERP-системи («1С», «BAS», рішення від «СКБ Контур»), продукти «Яндекс», «РусБІТехАстра», «Ред Софт», а також інженерне ПЗ (КОМПАС-3D, ЛОЦМАН, ВЕРТИКАЛЬ). Важливою зміною стало масове включення апаратного забезпечення — маршрутизаторів, комутаторів, міжмережевих екранів та шлюзів безпеки (зокрема лінійки ViPNet).

Простими словами (Оцінка ризику) Держава системно продовжує процес вилучення з інформаційного простору технологій, пов'язаних із підсанкційними особами. Використання заборонених програм чи апаратного забезпечення створює критичні передумови для несанкціонованого доступу до внутрішніх мереж та є прямим недотриманням законодавства у сфері кіберзахисту. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) наявність таких рішень у мережі несе два основні ризики. По-перше, виникає загроза компрометації інформаційно-комунікаційних систем (ІКС) та втрати конфіденційних даних. По-друге, виявлення такого ПЗ чи обладнання під час планових чи позапланових аудитів є прямою підставою для скасування статусу захищеності системи, що тягне за собою юридичну відповідальність керівництва та загрожує безперервності діяльності (business continuity) установи.

Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)

1. **Практичний крок:**
   - ІТ-підрозділам та Підрозділам захисту інформації та кіберзахисту доцільно завантажити актуальний Перелік із сайту ДССЗІ та провести позапланову інвентаризацію наявного програмного і апаратного забезпечення. У разі виявлення заборонених позицій, це обладнання необхідно негайно ізолювати від загальної мережі, а ПЗ — деінсталювати, запустивши процедуру міграції на безпечні аналоги.
2. **Відповідність нормативним вимогам**
   - Ці дії є прямим виконанням вимог Наказу ДССЗІ № 75, зокрема заходів ID.AM-01/02 (Інвентаризація систем та ПЗ), а також PR.PS-05 та PR.PS-02 (Заборона виконання несанкціонованого ПЗ та його видалення). Відсутність підсанкційних продуктів в інфраструктурі є абсолютною вимогою для підтримання цільового профілю безпеки в рамках системи управління ризиками (RMF) та проходження Авторизації систем відповідно до Постанови КМУ № 712.
3. **Стратегічне планування / Додаткова порада**
   - Керівникам установ варто ініціювати оновлення Стандартних операційних процедур щодо публічних закупівель. Доцільно зобов'язати ІТ-фахівців спільно з тендерними комітетами впровадити обов'язковий етап перевірки технічних специфікацій на предмет відсутності рішень із Переліку ДССЗІ ще до моменту оголошення закупівель, щоб уникнути фінансових та операційних втрат.

Додаткові матеріали

- Сайт Держспецзв'язку: Держспецзв'язку суттєво розширила Перелік забороненого до використання ПЗ та комунікаційного обладнання
- Сайт Держспецзв'язку: Перелік забороненого до використання ПЗ та обладнання розширено до 880 позицій

Соціальна інженерія — Сучасні фішингові кампанії проти українських установ



Суть оновлення За даними Держспецзв'язку, фішинг залишається одним із головних способів первинного проникнення в інформаційні системи. Зловмисники використовують штучний інтелект для підготовки переконливих повідомлень, фальшиві CAPTCHA-перевірки, моделі Phishing-as-a-Service, підроблені голосові повідомлення та різні канали комунікації: електронну пошту, SMS, телефонні дзвінки й месенджери. CERT-UA фіксувала розсилки шкідливих архівів під виглядом сертифікатів платформи Prometheus, перехоплення листування в Signal із подальшим поширенням DarkCrystal RAT, а також розповсюдження шкідливого програмного забезпечення під виглядом інструментів захисту від імені CERT-UA.

Простими словами (Оцінка ризику) Сучасний фішинговий лист може не містити помилок або очевидних ознак шахрайства. Повідомлення може надходити нібито від керівника, колеги, державного органу, постачальника або відомого сервісу. Відкриття вкладення, запуск архіву, введення пароля на підробленій сторінці або проходження фальшивої CAPTCHA може призвести до зараження робочої станції, викрадення облікових даних і подальшого поширення атаки всередині мережі установи.

Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)

1. **Практичний крок:**
   - Доцільно:
     - перевірити налаштування поштових шлюзів і карантину;
     - обмежити отримання вкладень RDP, MSI, HTA, JS та захищених паролем архівів від неперевірених відправників;
     - забезпечити багатофакторну автентифікацію для корпоративної пошти та критичних сервісів;
     - обмежити використання публічних поштових скриньок зі службових комп'ютерів;
     - регулярно проводити навчальні фішингові кампанії та інструктажі персонал
2. **Відповідність нормативним вимогам**
   - Навчання персоналу щодо розпізнавання соціальної інженерії відповідає заходу PR.AT-01 Наказу ДССЗІ №75. Захист поштового трафіку та блокування шкідливого коду охоплюються заходами PR.PT-02 і PR.PS-05. Виконання цих контролів є необхідним підґрунтям для забезпечення цільового профілю безпеки в рамках системи управління ризиками (RMF) та підтримки Авторизації систем згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - ҚДоцільно затвердити процедуру перевірки нетипових запитів щодо передачі даних, зміни платіжних реквізитів, запуску файлів або термінового виконання вказівок керівництва через альтернативний канал зв'язку.
   - Для зменшення ризику повторного використання паролів рекомендовано впровадити корпоративний менеджер паролів.

Додаткові матеріали

- Держспецзв'язку: Еволюція соціальної інженерії: Держспецзв'язку розповідає про сучасні фішингові кампанії

Кібергігієна — Загрози публічних мереж Wi-Fi та безпека віддаленого доступу



Суть оновлення Держспецзв’язку звертає увагу на критичні ризики використання відкритих публічних мереж Wi-Fi. Через відсутність належного шифрування трафіку зловмисники активно використовують такі мережі для перехоплення облікових даних та сесійних файлів (cookie) за допомогою атак типу «людина посередині» (Man-in-the-Middle) та створення фейкових точок доступу (Evil Twin), що імітують легітимні мережі закладів. Для мінімізації загроз регулятор рекомендує вимикати автоматичне підключення до мереж, уникати входу до чутливих сервісів без використання корпоративного VPN, завжди перевіряти наявність HTTPS-з'єднання та застосовувати двофакторну автентифікацію (2FA).

Простими словами (Оцінка ризику) Корпоративний периметр захисту закінчується там, де працівник підключає службовий пристрій до незахищеної мережі в кафе або транспорті. Якщо співробітник закладу охорони здоров'я або об'єкта критичної інфраструктури (ОКІ) авторизується в робочій пошті, системі електронного документообігу чи внутрішній системі через публічний Wi-Fi, зловмисники можуть непомітно перехопити його сесію. Маючи ці дані, ворог отримує легітимний віддалений доступ до інформаційно-комунікаційної системи (ІКС) установи. Це створює пряму загрозу витоку конфіденційних даних та зупинки надання послуг, що безпосередньо впливає на безперервність діяльності (business continuity).

Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)

1. **Практичний крок:**
   - ІТ-підрозділам доцільно налаштувати політики управління мобільними пристроями (MDM) та групові політики (GPO) таким чином, щоб примусово заборонити службовій техніці автоматичне підключення до відкритих Wi-Fi мереж. Для забезпечення безпечної віддаленої роботи необхідно впровадити технологію "Always On VPN", яка автоматично шифрує весь трафік доступу до корпоративних ресурсів незалежно від мережі перебування.
2. **Відповідність нормативним вимогам**
   - Захист каналів віддаленого доступу та шифрування трафіку є прямими вимогами Наказу ДССЗІ № 75 (категорія PR.AC-03: Управління віддаленим доступом). Крім того, інструктаж персоналу щодо роботи з публічними мережами (PR.AT-01) є обов'язковим елементом системи управління ризиками (RMF) та критичною умовою для успішного проходження Авторизації систем згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - Керівникам установ варто ініціювати розробку та затвердження Стандартних операційних процедур щодо правил віддаленої роботи (telework). Цей документ має чітко забороняти доступ до критичних ресурсів чи баз даних без використання захищених корпоративних каналів зв'язку.

Додаткові матеріали

- Держспецзв’язку: Кібергігієна: чекліст безпечного використання публічного Wi-Fi

Загрози кібершпигунства — Кампанії Gamaredon і Turla проти українських установ



Суть оновлення Російські кіберугруповання Gamaredon і Turla продовжують цілеспрямовані атаки на державні, військові та інші українські організації. Gamaredon використовує фішингові кампанії, техніку HTML smuggling, PowerShell-модулі сімейства Ptero, зараження USB-накопичувачів і спільних мережевих папок. Для приховування управління шкідливим програмним забезпеченням застосовуються легітимні сервіси Telegra.ph, Dropbox, Mastodon та GoFile. Угруповання Turla застосовує багатокомпонентний .NET-бекдор STOCKSTAY, який маскується під легітимні програми. Зараження здійснюється через фішингові листи з файлами RDP, MSI або RAR. Для розміщення шкідливого навантаження використовуються скомпрометовані WordPress-сайти й репозиторії GitHub. В обох кампаніях зафіксовано експлуатацію вразливості WinRAR CVE-2025-8088.

Простими словами (Оцінка ризику) Мета таких атак — не одноразове зараження комп'ютера, а тривале приховане перебування в інфраструктурі установи. Після первинного проникнення зловмисники намагаються поширитися через спільні папки, USB-накопичувачі та облікові записи працівників, збирати документи, робити знімки екрана, викрадати дані та підтримувати резервні канали доступу. Використання популярних хмарних сервісів і сайтів ускладнює виявлення, оскільки шкідливий трафік може виглядати як звичайна активність користувачів.

Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)

1. **Практичний крок:**
   - Необхідно:
     - перевірити версії WinRAR і встановити оновлення, що усуває CVE-2025-8088;
     - обмежити запуск PowerShell, VBScript та інших скриптів для стандартних користувачів;
     - фільтрувати вкладення RDP, MSI, HTA та архіви з паролями;
     - обмежити використання несанкціонованих USB-накопичувачів;
     - контролювати доступ до нерегламентованих хмарних сервісів;
     - перевіряти аномальне використання WebSocket та інших зашифрованих каналів;
     - передати актуальні індикатори компрометації до SIEM, EDR/XDR та засобів мережевого захисту.
2. **Відповідність нормативним вимогам**
   - Блокування несанкціонованих скриптів та жорсткий контроль конфігурацій є прямими вимогами Наказу ДССЗІ № 75 (заходи PR.PT-01: Управління конфігураціями кінцевих пристроїв та PR.PS-05: Заборона встановлення та виконання несанкціонованого програмного забезпечення). Регулярне оновлення ПЗ (Patch Management) є обов'язковим елементом підтримання цільового профілю безпеки в рамках системи управління ризиками (RMF) для Авторизації систем відповідно до Постанови КМУ № 712.
3. **Стратегічне планування**
   - Доцільно впроваджувати рішення EDR/XDR, які виявляють виконання коду в оперативній пам'яті, нетипову міжпроцесну взаємодію, спроби бокового переміщення мережею та встановлення прихованих каналів управління.
   - Окремо необхідно регламентувати використання USB-накопичувачів, хмарних сховищ, сервісів обміну файлами та засобів виконання сценаріїв.

Додаткові матеріали

- **The Hacker News: Google Details Turla's New STOCKSTAY Backdoor Used in Ukraine Espionage Attacks**
- The Hacker News: Gamaredon Expands Ukraine Attacks with New Malware and Cloud Service Abuse

Соціальна інженерія — Російські спецслужби викрадають акаунти в месенджерах через фейкову службу підтримки



Суть оновлення Служба безпеки України (СБУ) спільно з ФБР США викрили довготривалу кібершпигунську кампанію російських спецслужб, спрямовану на урядовців, військовослужбовців, політиків та громадян в Україні, Європі та США. Зловмисники (зокрема угруповання Star Blizzard, UAC-0195 та UAC-0185) масово розсилають SMS-повідомлення, маскуючись під офіційних ботів служби підтримки месенджерів (Signal, WhatsApp). Вони вимагають від користувачів розкрити облікові дані, PIN-коди або ключі відновлення (backup recovery keys). Метою атак є викрадення конфіденційної військової, політичної, економічної інформації та персональних даних. Паралельно CERT-UA фіксує активність пробілоруського угруповання Ghostwriter (UAC-0057), яке використовує вже скомпрометовані акаунти для цілеспрямованої розсилки вірусу-стілера OYSTERBLUES державним організаціям.

Простими словами (Оцінка ризику) Атаки через популярні месенджери стали одним із головних інструментів ворожої розвідки. Зловмисники створюють ілюзію технічної проблеми з акаунтом та, використовуючи психологічний тиск від імені "служби підтримки", змушують користувачів самостійно віддати ключі доступу. Для закладів охорони здоров'я та об'єктів критичної інфраструктури (ОКІ) злам месенджера працівника означає не лише ризик витоку службового листування. Скомпрометований акаунт одразу використовується ворогами як довірене джерело для розсилки шкідливих файлів іншим співробітникам. Це створює пряму загрозу проникнення вірусів у внутрішні інформаційно-комунікаційні системи (ІКС), що може призвести до масштабного витоку реєстрів та тривалого порушення безперервності діяльності (business continuity) установи.

Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)

1. **Практичний крок:**
   - Підрозділам захисту інформації доцільно провести цільовий інструктаж персоналу щодо суворої заборони розголошення кодів підтвердження, PIN-кодів та ключів відновлення доступу.
   - Працівникам необхідно регулярно перевіряти активні сесії в месенджерах і примусово виходити з невідомих підключень.
   - Варто категорично уникати сканування QR-кодів від невідомих користувачів, а також не переходити за підозрілими посиланнями та не відкривати файли з сумнівних чатів.
   - Рекомендується забезпечити обов'язкове ввімкнення двофакторної автентифікації (2FA) для всіх робочих комунікацій.
2. **Відповідність нормативним вимогам**
   - Забезпечення обізнаності персоналу щодо ризиків соціальної інженерії (категорія PR.AT-01: Обізнаність та навчання) є невід'ємною вимогою Наказу ДССЗІ № 75. Систематичний контроль автентифікації та навчання працівників є базовою умовою для підтримання цільового профілю безпеки в межах системи управління ризиками (RMF) та успішної Авторизації ІКС згідно з Постановою КМУ № 712.
3. **Стратегічне планування**
   - Керівникам установ варто ініціювати розробку та затвердження Стандартних операційних процедур (СОП), що чітко регламентують використання месенджерів у службових цілях. Доцільно впровадити в корпоративну культуру концепцію «нульової довіри» (Zero Trust) до будь-яких повідомлень, які вимагають термінової передачі даних, навіть якщо вони надходять від знайомих контактів (адже акаунт відправника може бути вже скомпрометований).

Додаткові матеріали

- The Hacker News: Ukraine Says Russian Intelligence Used Fake Support Texts to Steal Messaging Credentials

Фізична безпека пристроїв — Ризики офлайн-зламу девайсів у зоні бойових дій через криміналістичний софт ворога



Міжнародна дослідницька група Citizen Lab опублікувала звіт, який підтверджує, що російські спецслужби та силові структури продовжують успішно використовувати криміналістичні комплекси Cellebrite (UFED Physical Analyzer та UFED 4PC) для зламу вилучених мобільних пристроїв. Це відбувається попри офіційну заяву виробника про припинення продажів та підтримки в рф. Дослідження довело, що раніше встановлене апаратне забезпечення Cellebrite повноцінно функціонує в автономному (офлайн) режимі без зв'язку з серверами розробника. За допомогою цих інструментів ворог викачує дані з месенджерів (Signal, WhatsApp, Telegram, Viber), вилучає сесійні токени та формує соціальні графи жертв. Отримані списки контактів згодом передаються хакерським угрупованням (зокрема пов'язаному з ФСБ угрупованню COLDRIVER) для організації наступних точкових фішингових кампаній. Водночас зафіксовано, що увімкнене шифрування диска в поєднанні з відсутністю пароля блокує можливості криміналістичного обладнання для зчитування інформації.

Простими словами (Оцінка ризику) Для медичного персоналу, евакуаційних бригад та військовослужбовців, які працюють безпосередньо в зоні бойових зіткнень, ризик потрапляння пристроїв у руки ворога є критично високим. Російські спецслужби не намагаються підбирати паролі вручну — вони використовують готові криміналістичні станції UFED, які вже розгорнуті в їхніх польових і тилових пунктах. Якщо смартфон потрапляє до рук окупантів у ввімкненому стані або захищений простим чотиризначним кодом, ворог за лічені хвилини отримає доступ до координат, внутрішніх чатів евакуації, даних про поранених, а головне — до списків контактів. Злам одного телефону медика чи координатора автоматично створює базу цілей для наступних ворожих операцій, а також полегшує підготовку персоналізованого фішингу проти всього підрозділу чи установи.

Рекомендовані напрями для опрацювання (Для керівників та Підрозділів кіберзахисту)

1. **Практичний крок:**
   - ІТ-підрозділам та Підрозділам захисту інформації та кіберзахисту необхідно забезпечити максимальне технічне посилення конфігурацій безпеки всіх мобільних пристроїв, що використовуються в зоні підвищеного ризику. Обов'язково встановити складні літерно-цифрові паролі (мінімум 8–10 символів) замість графічних ключів чи коротких PIN-кодів. На пристроях Apple примусово активувати Lockdown Mode, а на пристроях Android — режим максимального захисту (Advanced Protection). Персонал має суворо дотримуватися правила: перед входом у зону потенційного бойового зіткнення пристрій повинен бути повністю вимкнений (Power Off), щоб перевести криптографічні ключі пам'яті в заблокований стан, який суттєво ускладнює роботу криміналістичних комплексів. У разі повернення раніше вилученого або втраченого пристрою, його заборонено підключати до внутрішньої мережі установи до проходження глибокого аналізу, а всі паролі облікових записів мають бути негайно змінені.
2. **Відповідність нормативним вимогам**
   - Запровадження механізмів криптографічного захисту інформації в мобільних точках, контроль конфігурацій пристроїв та проведення обов'язкових інструктажів з кібергігієни в умовах воєнного стану безпосередньо відповідають вимогам Наказу Наказу ДССЗІ № 75 (зокрема функції PR.DS-01 щодо захисту даних у стані спокою та PR.PT-03 щодо управління мобільними пристроями — MDM). Ці кроки є невід'ємною частиною підтримки цільового профілю безпеки відповідно до Постанови КМУ № 712 та системи RMF.
3. **Стратегічне планування**
   - Керівникам установ спільно з підрозділами кіберзахисту рекомендується розробити та затвердити галузеві Стандартні операційні процедури (СОП) для персоналу, який відряджається або працює в прифронтових районах. Необхідно впровадити обов'язкове використання систем централізованого керування мобільними пристроями (MDM) з можливості віддаленого знищення всіх даних (remote wipe) у разі втрати зв'язку з апаратом або за сигналом тривоги.

Додаткові матеріали

- The Hacker News: Russia Used Cellebrite on Jailed Activist's iPhone Months After Sales Cutoff