Реагування на кіберінциденти, кібератаки та кіберзагрози

ЗАКОН УКРАЇНИ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

Загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози, а також механізм координації та взаємодії між суб'єктами національної системи реагування та суб'єктами забезпечення кібербезпеки визначаються в **Національному плані реагування на кіберінциденти, кібератаки та кіберзагрози** (затверджено постановою Кабінету Міністрів України від 26 листопада 2025 р. № 1533).

Підрозділ з кіберзахисту

Структурний підрозділ або група осіб суб'єкта забезпечення кібербезпеки, що виконує завдання із забезпечення кібербезпеки та кіберзахисту й здійснює захист інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, об'єктів критичної інформаційної інфраструктури.

Департаменту кібербезпеки СБУ. Служба безпеки створила регіональні центри забезпечення кібербезпеки в усіх областях України.

Власна команда реагування (CSIRT)

Структурний підрозділ або група осіб суб'єкта забезпечення кібербезпеки, що у межах повноважень виконує завдання із реагування на кіберінциденти, кібератаки та кіберзагрози.

Національна система реагування

Комплекс правових та організаційно-технічних заходів і засобів, спрямованих на швидке виявлення кіберінцидентів та кібератак, ідентифікацію та аналіз кіберзагроз, оперативне інформування про них, вжиття заходів для мінімізації їх наслідків, усунення виявлених вразливостей, а також відновлення сталого і надійного функціонування систем.

Відповідно до ст. 5-1 Закону України «Про основні засади забезпечення кібербезпеки України» в органах державної влади утворюються підрозділи з кіберзахисту та призначаються керівники з кіберзахисту, а в органах місцевого самоврядування — особи, які виконують їхні функції та завдання.

Підготовка до реагування на кіберінциденти, кібератаки та кіберзагрози

Реагування розпочинається з етапу підготовки, під час якого суб'єктами проводяться заходи з вивчення та дослідження існуючих видів кіберінцидентів, кібератак та кіберзагроз, розроблення методів і механізму запобігання та протидії можливим кіберінцидентам та кібератакам.

1

Планування заходів

Планування заходів з реагування на постійній та системній основі з урахуванням результатів управління ризиками кібербезпеки.

2

Взаємодія підрозділів

Забезпечення взаємодії між керівниками з кіберзахисту, підрозділами з кіберзахисту, власними командами CSIRT та суб'єктами національної системи реагування.

3

Стандартні процедури

Розроблення та підтримання в актуальному стані стандартних операційних процедур для реагування на різні категорії кіберінцидентів з урахуванням методичних рекомендацій Адміністрації Держспецзв'язку.

4

Навчання персоналу

Організація регулярного навчання з питань реагування диференційовано залежно від функціональних обов'язків та з урахуванням професійної кваліфікації співробітників.

5

Технічна інтеграція

Створення технічних можливостей підключення власних систем до засобів і технічних систем реагування суб'єктів національної системи реагування, зокрема до системи Державного центру кіберзахисту Держспецзв'язку.

Виявлення, аналіз та інформування про кіберінциденти, кібератаки та кіберзагрози

На цьому етапі проводиться постійний моніторинг систем, збір інформації про події кібербезпеки, підтвердження та первинна обробка подій, виявлення індикаторів компрометації та підозрілої активності, ідентифікація та аналіз кіберзагроз, а також інформування про кіберінциденти, кібератаки та кіберзагрози.

Рівні критичності кіберінцидентів

Рівень 0 — Некритичний (білий)

Кіберінцидент не загрожує сталому, надійному та штатному режиму функціонування систем.

Рівень 1 — Низький (зелений)

Безпосередньо загрожує функціонуванню систем, але не загрожує захищеності інформації та даних.

Рівень 2 — Середній (жовтий)

Загрожує функціонуванню систем, створює передумови для порушення захищеності інформації та припинення функцій критичної інфраструктури.

Рівень 3 — Високий (помаранчевий)

Порушується захищеність інформації, виникають потенційні загрози для національної безпеки, соціальної сфери, національної економіки та критичної інфраструктури.

Рівень 4 — Критичний (червоний)

Загрожує кільком системам, виникають реальні загрози для національної безпеки і оборони, соціальної сфери, національної економіки та критичної інфраструктури.

Рівень 5 — Надзвичайний (чорний)

Загрожує значній кількості систем, виникають невідворотні загрози для повноцінного функціонування держави або загроза життю людей.

Строки інформування про значні кіберінциденти

1. **Попереднє повідомлення**
   Протягом **24 годин** після виявлення значного кіберінциденту
2. **Поточний звіт**
   Протягом **72 годин** після виявлення кіберінциденту
3. **Остаточний звіт**
   Протягом **одного місяця** після інциденту

Інформування здійснюється безперервно в режимі, наближеному до реального часу, з використанням платформи обміну інформацією та механізму «єдиного вікна» з дотриманням протоколу TLP, визначеного Адміністрацією Держспецзв'язку.

Стримування, усунення наслідків та відновлення після кіберінцидентів

Під час цього етапу суб'єкти забезпечення кібербезпеки самостійно або разом із суб'єктами національної системи реагування вживають заходів до зниження негативного впливу кіберінциденту, кібератаки, запобігання порушенню безпеки та забезпечення сталого функціонування систем. З початку повномасштабного вторгнення рф фахівці ДКІБ нейтралізували понад 14 тисяч масштабних кібератак та кіберінцидентів на ресурси центральних органів влади та критичної інфраструктури нашої держави. Зокрема протидіють проникненню та блокуванню ворогом важливих військових та урядових мереж, відбивати DDoS-навали, фішингові кампанії, протистояти кібершпигунству та цифровому тероризму. (документальний фільм «Кіберщит України»)

Рекомендації CERT-UA / CSIRT

Після отримання та опрацювання повідомлень про кіберінциденти, кібератаки, кіберзагрози надаються рекомендації щодо можливих заходів реагування та технічної підтримки (у разі потреби).

Технічне дослідження

Аналіз обставин виникнення кіберінциденту, збір технічних даних зі скомпрометованих або уражених систем та їх дослідження, формування індикаторів кіберзагрози, виявлення додаткових уражених систем.

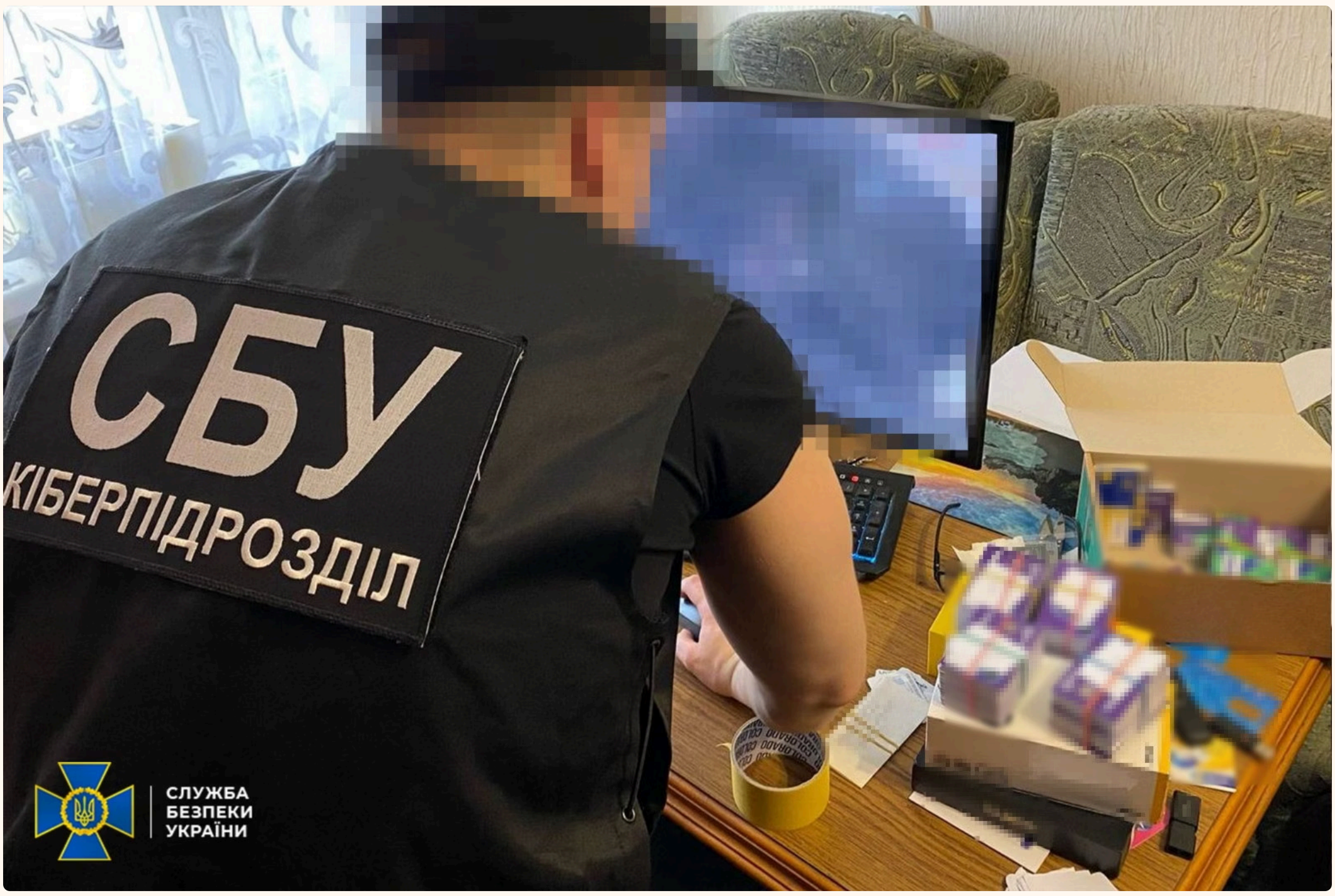
Передача до СБУ

Якщо під час технічного дослідження виявлено ознаки кримінального правопорушення, така інформація невідкладно — **протягом однієї години** — передається до СБУ.

КЕЙС РЕАЛЬНИЙ ВИПАДОК

Ботоферма у Житомирі: затримання організатора інформдиверсій

Служба безпеки та Національна поліція затримали у Житомирі організатора підпільної ботоферми, яку рашисти використовували для проведення інформдиверсій проти України.



Масштаб діяльності

Щомісяця продавав до країни-агресора понад **3 000** фейкових сторінок у Телеграмі.

Схема створення акаунтів

Створював «підставні» акаунти на мобільні номери українських операторів.

Канали збуту

Продавав акаунти на спеціалізованих ворожих онлайн-платформах.

Основні клієнти

Представники російських спецслужб.

Призначення фейкових акаунтів

Поширення дезінформації про Сили оборони та анонімні повідомлення про «мінування» об'єктів.

Що заблоковано

Майже **20 000** фейкових інтернет-профілів.

Результати операції

- Вилучено комп'ютерну техніку
- Вилучено USB-хаби з модемами
- Вилучено телефони
- Вилучено майже **2 000** сім-карт
- Повідомлено про підозру за ч. 2 ст. 361 КК України

Кваліфікація: несанкціоноване втручання в роботу інформаційних систем за попередньою змовою групою осіб.

Аналіз ефективності заходів реагування на кіберінциденти, кібератаки та кіберзагрози

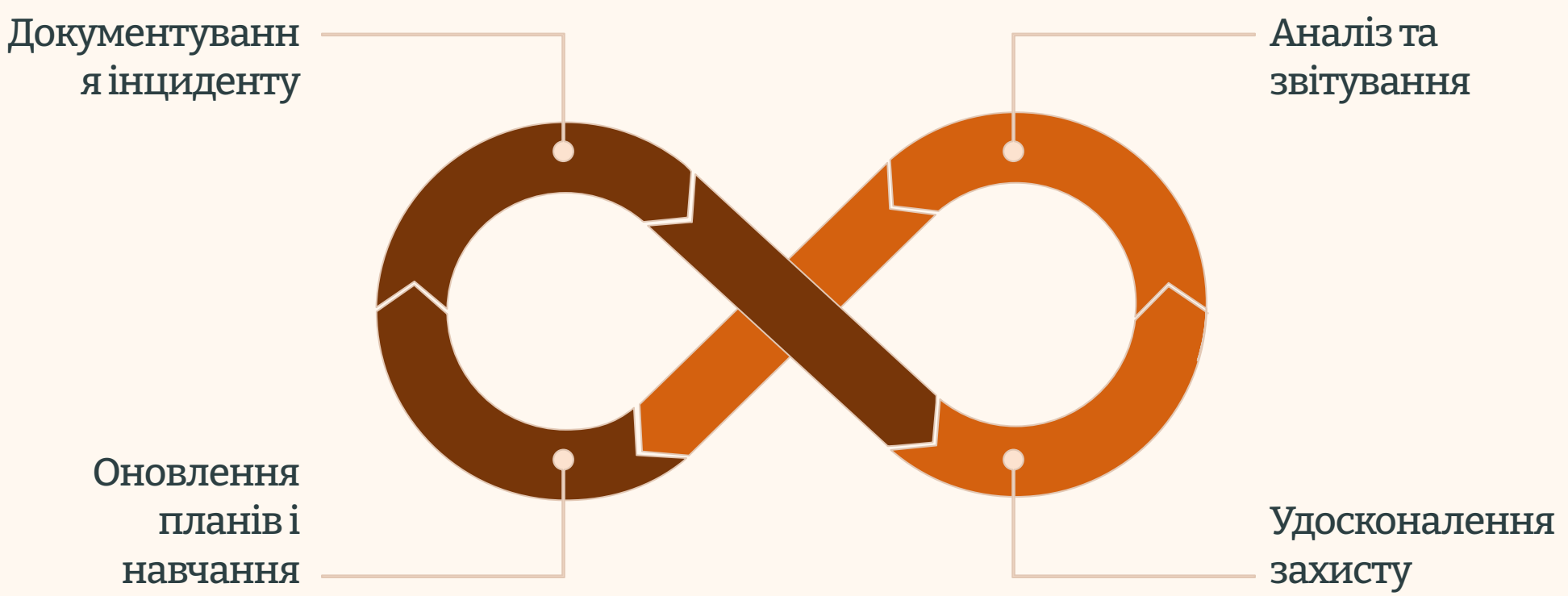
За результатами вжиття заходів реагування суб'єкти забезпечення кібербезпеки у взаємодії із CERT-UA та/або Ситуаційним центром забезпечення кібербезпеки СБУ, та/або відповідною галузевою/регіональною командою CSIRT проводять аналіз ефективності реагування.

Під час аналізу забезпечується:

- Документування інциденту шляхом формування звіту про реагування на кіберінцидент, кібератаку або кіберзагрозу
- Інформування CERT-UA та Ситуаційного центру СБУ або відповідної галузевої/регіональної команди CSIRT
- Удосконалення захисних механізмів систем і мереж
- Перегляд внутрішньої документації та політик безпеки для запобігання подібним інцидентам у майбутньому
- Застосування набутого досвіду для покращення управління майбутніми кіберінцидентами та кібератаками

Результати аналізу враховуються при:

- → Оновленні планів реагування на кіберінциденти, кібератаки або кіберзагрози
- → Оновленні внутрішніх політик кібербезпеки та плану кіберзахисту
- → Плануванні і проведенні навчань, тренувань та інших заходів підготовки персоналу



Служба безпеки спільно з ФБР, контррозвідувальними органами Республіки Польща та правоохоронними органами ЄС провела скоординовану кібероперацію з нейтралізації розвідувальної діяльності ворога на території України та держав-партнерів.

За результатами міжнародної кібероперації викрито численні факти «зламу» російською воєнною розвідкою (більш відомою як гру) офісних, домашніх Wi-Fi роутерів українців та іноземних громадян (так зване SOHO-обладнання).

За матеріалами розслідування, російські спецслужбісти «полювали» на роутери, які не відповідали сучасним протоколам безпеки. Після «проникнення» до вразливих інтернет-пристроїв рашисти перенаправляли їх трафік через заздалегідь розгорнуту мережу DNS-серверів (перетворюють назви ресурсів Інтернету в їх IP-адреси, які однозначно ідентифікують сервер призначення).

У такий спосіб вони ставали «посередниками» в онлайн-просторі, щоб збирати паролі, токени автентифікації та іншу чутливу інформацію, включно з електронними листами, які за нормальних умов захищені криптографічними протоколами SSL (secure sockets layer) та TLS (transport layer security). Отримані відомості ворог планував використати для здійснення кібератак, інформдиверсій та збору розвідувальної інформації.

У зоні особливої уваги російської спецслужби була інформація, якою обмінюються співробітники та військовослужбовці держаних органів, підрозділів Сил оборони України, підприємств оборонно-промислового комплексу.

За результатами проведеної спільної кібероперації вдалося заблокувати понад 100 серверів та вивести з-під контролю ворога сотні маршрутизаторів лише в Україні, що суттєво послабило розвідувальні спроможності військової розвідки рф, запобігло знищенню обладнання на програмному рівні. Наразі тривають комплексні заходи Служби безпеки України та її західних партнерів для притягнення до відповідальності всіх осіб, причетних до кіберзлочинів.

СБУ рекомендує всім власникам роутерів актуалізувати для себе модель та поточну версію програмного забезпечення пристрою, наявність актуальних оновлень безпеки до неї, їх невідкладно імплементувати. У разі відсутності підтримки з боку виробника наполегливо пропонуємо замінити роутер на сучаснішу модель, у тому числі від іншої компанії. Після оновлення необхідно обов'язково змінити пароль доступу до пристрою, вимкнути можливість доступу до його панелі керування з мережі «Інтернет», перевірити налаштування та видалити підозріле. **https://ssu.gov.ua/novyny/sbu-fbr-ta-pravookhoronni-orhany-yes-vykryly-hru-rf-na-masshtabnomu-shpyhuvanni-za-hromadianamy-yes-ssha-ta-ukrainy-cherez-khaknuti-wifi-routery**

Служба безпеки затримала у Києві ще одного російського агента. Ним виявися завербований фсб 40-річний працівник відділу інформаційної безпеки одного з комерційних банків столиці.

За матеріалами кіберфахівців СБУ, фігурант збирав для ворога персональні дані клієнтів фінустанови серед воїнів Сил оборони та військових волонтерів. Ці дані окупанти могли використати для підготовки терактів, інформаційних диверсій та вербувальних операцій проти українських захисників. Співробітники СБУ завчасно викрили агента, задокументували його розвідактивність і затримали за місцем проживання. Під час обшуку в нього вилучено чотири смартфони, змінні сім-карти для конспірації і три ноутбуки, на яких він накопичував особисті дані потенційних «цілей». Також на гаджетах затриманого виявлено його контакти з фсб. З*а матеріалами справи, банківський працівник потрапив до уваги рашистів через свою активність у забороненій соцмережі.*

Після вербування агент отримав від куратора з рф «тестові» завдання на проведення дорозвідки поблизу пунктів базування Сил оборони у Києві. Для цього банкір у вихідні обходив місцевість і фотографував будівлі, які, на його думку, могли використовувати українські захисники. Згодом він отримав завдання на збір інформації про клієнтів фінустанови з-поміж військових і волонтерів, що відкривали рахунки на допомогу для ЗСУ.

Також він мав передати окупантам координати резервного дата-центру, на якому зберігається база даних банку та його користувачів.

Слідчі СБУ повідомили агенту про підозру за ч. 2 ст. 111 Кримінального кодексу України (державна зрада, вчинена в умовах воєнного стану).

Критерії віднесення інформації про кіберінцидент до інформації з обмеженим доступом

Відкрита інформація

Інформація про кіберінцидент, кібератаку щодо систем та про їх наслідки **є відкритою** інформацією.

Інформація про **індикатори кіберзагроз**, отримана під час реагування, також є відкритою і поширюється у порядку обміну інформацією, визначеному Адміністрацією Держспецзв'язку.

Інформація з обмеженим доступом

Інформація про характер, технічні та інші деталі кіберінциденту, кібератаки належить до інформації **з обмеженим доступом**, якщо вона відповідає хоча б одному з критеріїв.

Критерії обмеженого доступу

Містить неоприлюднені відомості про **архітектуру, конфігурацію, технічні характеристики або вразливості** системи, щодо якої здійснено кіберінцидент, кібератаку.

Містить відомості про **скомпрометовані облікові записи, системи, вектори реалізації** кіберінцидентів або масштаби впливу, які можуть бути використані для повторних атак.

Безпосередньо стосується або дає змогу встановити перебіг **оперативно-розшукових, контррозвідувальних заходів, слідчих дій або розвідувальної діяльності.**

Надана з вимогою обмеження доступу **міжнародними, міжурядовими чи приватними партнерами** суб'єктів національної системи реагування.

Дає змогу **ідентифікувати фізичних чи юридичних осіб** або містить персональні дані осіб, пов'язаних з кіберінцидентом, кібератакою.

Підстави для розкриття інформації з обмеженим доступом

У межах національної системи реагування

Якщо розкриття є обґрунтовано необхідним для виконання повноважень суб'єктів, залучених до реагування на кіберінциденти та кібератаки або їх розслідування.

За погодженням із суб'єктом

За погодженням із суб'єктом національної системи реагування, який прийняв рішення про обмеження доступу, у разі потреби забезпечення координації реагування або розслідування.

Для запобігання подальшим атакам

Коли розкриття є необхідним для запобігання подальшим кіберінцидентам і кібератакам або мінімізації їх наслідків.

⚠ Розкриття здійснюється за умови, якщо обробка інформації буде здійснюватися з визначеною метою розкриття, а також якщо це не створює загроз національній безпеці України, не порушує вимог законодавства про захист персональних даних, комерційної, банківської, державної таємниці або інших вимог захисту інформації.

Порядок публічного інформування або звітування про реагування на кіберінциденти та кібератаки

Власники або розпорядники систем у взаємодії з відповідною галузевою або регіональною командою CSIRT, а у разі її відсутності — з CERT-UA, здійснюють публічне інформування про реагування на кіберінциденти, кібератаки та усунення їх наслідків, забезпечуючи своєчасність і достовірність повідомлень.

Коли здійснюється публічне інформування?

Публічне інформування здійснюється щодо кіберінцидентів, кібератак **від середнього рівня критичності та вище** (рівень 2 і вище).

Як здійснюється?

Шляхом публікації спільних прес-релізів, офіційних повідомлень або заяв на інформаційних ресурсах відповідної команди CSIRT або CERT-UA та власника або розпорядника системи.

Обмеження публічного інформування

- Лише в тому обсязі, який **не створює додаткових загроз** національній безпеці та не заважає реагуванню.
- У разі реагування СБУ у сфері державної безпеки — **за погодженням з відповідним підрозділом СБУ.**
- Якщо факт кіберінциденту є предметом досудового розслідування — **лише з письмового дозволу слідчого або прокурора.**

Публічне звітування

Форма звітів

Узагальнені аналітичні звіти, що можуть містити аналітичну, технічну, статистичну інформацію про характер загроз, основні вектори атак, тенденції у сфері кібербезпеки та ефективність заходів реагування.

Хто формує звіти?

Суб'єкти національної системи реагування. Публікуються у відкритому або обмеженому доступі залежно від змісту.

Мета публікації

Інформування суб'єктів забезпечення кібербезпеки, громадськості та міжнародних партнерів, а також підвищення прозорості та обізнаності щодо кіберзагроз.

Особливості для Міноборони

Особливості публічного інформування щодо систем Міноборони визначаються Міноборони разом з Генеральним штабом ЗСУ та погоджуються з Адміністрацією Держспецзв'язку та СБУ.

Джерела та нормативна база

НОРМАТИВНО-ПРАВОВІ АКТИ

Закон України «Про основні засади забезпечення кібербезпеки України»

Основний законодавчий акт, що визначає правові та організаційні засади забезпечення кібербезпеки України, у тому числі статус підрозділів з кіберзахисту та команд реагування.

Постанова КМУ від 26 листопада 2025 р. № 1533

Національний план реагування на кіберінциденти, кібератаки та кіберзагрози. Також затверджує критерії віднесення інформації до обмеженого доступу та порядок публічного інформування.
https://zakon.rada.gov.ua/laws/show/1533-2025-п/ed20251126#n17

Постанова КМУ від 26 листопада 2025 р. № 1516

«Про затвердження Порядку призначення керівника з кіберзахисту на посаду в органі державної влади»

Наказ Адміністрації Держспецзв'язку від 03.12.2025 № 798

«Про затвердження Методичних рекомендацій щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту в органах державної влади, а також до відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органах місцевого самоврядування»

Усі нормативні акти доступні на офіційному порталі законодавства України: zakon.rada.gov.ua