Державна служба спеціального зв’язку
та захисту інформації України

ДЕРЖНДІ · 5 ЦЕНТР· 2026

Кібергігієна:

як захистити свої дані від кіберзагроз

5 Центр ДержНДІ технологій кібербезпеки

Ландшафт сучасних кіберзагроз

Виклики для державних установ у 2024-2025 роках

37,4 %

Зростання кібератак (2024-2025)

https://cip.gov.ua

184 дні

Середній час виявлення інциденту

https://www.totalassure.com

89%

Атак починаються з фішингу

https://zensec.co.uk

APT-групи

Цілеспрямовані тривалі атаки на критичну інфраструктуру

DDoS-атаки

Виведення з ладу державних сервісів

Програми-вимагачі

Шифрування даних з вимогою викупу

Insider threats

Внутрішні загрози від персоналу

Основи кібергігієни

Базові правила цифрової безпеки для кожного співробітника

Регулярне оновлення ПЗ

Встановлення патчів не пізніше 48 годин після виходу критичних оновлень

Мінімальні привілеї

Принцип least privilege – доступ лише до необхідних ресурсів

Резервне копіювання

Правило 3-2-1: 3 копії, 2 носії, 1 поза периметром

Блокування сесій

Автоблокування робочої станції через 5 хвилин бездіяльності

Заборонені дії

Використання особистих USB-носіїв, несанкціонованого ПЗ

Публічні мережі

Підключення до корпоративних ресурсів без VPN

Zero Trust та операційна безпека

Zero Trust

Модель «Нульової довіри»

- Жоден запит, файл чи посилання не є безпечними за замовчуванням
- Повна верифікація перед будь-яким доступом до ресурсів
- Звичайний обліковий запис – для щоденної роботи
- Привілейований обліковий запис – виключно для адміністративних дій

OPSEC

Мінімізація цифрового сліду

- Не розголошувати внутрішні регламенти та структуру мережі
- Не публікувати фото робочих місць і документів у соцмережах
- Не використовувати робочу пошту на сторонніх сервісах
- Розмежовувати службове та приватне цифрове середовище

Парольна безпека та багатофакторна автентифікація

ВИМОГИ ДО ПАРОЛЯ

- ✓ Мінімум 12 символів
- ✓ Великі та малі літери
- ✓ Цифри та спецсимволи (@, #, $)
- ✓ Не містить персональних даних
- ✓ Унікальний для кожного сервісу
- ✓ Зміна кожні 90 днів (критичні системи)
- ✓ Заборонені словникові слова

БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ (MFA)

Апаратні ключі (FIDO2/WebAuthn)
Найвищий рівень захисту – обов'язково для адміністраторів

TOTP-застосунки (Authy, Google Auth)
Одноразові коди – рекомендовано для всіх

SMS-коди
Допустимо, але вразливо до SIM-swapping

Біометрія
Додатковий фактор – не замінює основний

Фішинг та соціальна інженерія

До 89% успішних атак починаються з фішингового листа або дзвінка – ключова загроза для держорганів

Спір-фішинг

Цільові листи під конкретну особу або установу з персоналізованим змістом

Вішинг

Телефонні дзвінки від «служби безпеки», «IT-відділу» або керівництва

Смішинг

Шахрайські SMS з посиланнями на підроблені сторінки держсервісів

Претекстинг

Створення правдоподібної легенди для отримання конфіденційних даних

ОЗНАКИ ПІДОЗРІЛОГО ЛИСТА:

• Невідомий відправник • Терміновість та тиск • Незвичний домен • Посилання відрізняється від тексту • Прохання надати дані

Безпека мобільних пристроїв

MDM-рішення

Централізоване управління корпоративними пристроями, примусова криптографія

Офіційні магазини

Встановлення застосунків лише з App Store / Google Play. Заборона sideloading

Контейнеризація

Ізоляція робочих даних від особистих застосунків та файлів

PIN/Біометрія

6-значний PIN або біометрія + автоблокування через 2 хвилини

Шифрування

Повне шифрування диска обов'язкове для всіх службових пристроїв

Оновлення ОС

Обов'язкове встановлення оновлень безпеки впродовж 7 днів

Remote Wipe

Видалення даних при втраті або крадіжці пристрою

Wi-Fi безпека

Заборона підключення до відкритих Wi-Fi мереж без VPN

Безпечна робота у мережі

Зонування мережевої інфраструктури

DMZ Демілітаризована зона	Веб-сервери, поштові шлюзи – обмежений доступ ззовні та всередину
Корпоративна мережа Внутрішній периметр	АРМ співробітників, внутрішні сервери – строгий контроль доступу
Сегмент управління Out-of-band	Мережеве обладнання – ізольований сегмент для адміністрування

Принципи міжмережевого екрану: Default Deny • Least Access • Deep Packet Inspection • Логування всіх подій

Захист від шкідливого програмного забезпечення

ТИПИ ШКІДЛИВОГО ПЗ

Ransomware

Шифрування файлів з вимогою викупу у криптовалюті

Spyware

Збір конфіденційних даних, перехоплення клавіатури та екрану

Rootkit

Приховане встановлення на рівні ОС, обхід засобів захисту

Trojan

Корисне ПЗ із прихованою шкідливою функцією

ЗАСОБИ ЗАХИСТУ

EDR-рішення

Постійний моніторинг поведінки процесів, автоматична ізоляція загрозливих хостів

Антивірус нового покоління

ML-аналіз, захист від zero-day атак, хмарні сигнатури в реальному часі

Application Whitelisting

Дозвіл лише схваленого ПЗ, блокування всього іншого

Sandbox-аналіз

Перевірка підозрілих файлів у ізольованому середовищі

Управління інцидентами кібербезпеки

01 Виявлення

Моніторинг SIEM, сповіщення від систем захисту, повідомлення персоналу

02 Класифікація

Визначення критичності, впливу, категорії за класифікатором CERT-UA

03 Стримування

Ізоляція скомпрометованих систем, блокування трафіку, збереження доказів

04 Ліквідація

Видалення загрози, відновлення систем, патчинг вразливостей

05 Відновлення

Поетапне повернення систем у роботу, верифікація цілісності

06 Аналіз

Post-mortem, звіт CERT-UA, оновлення процедур захисту

Безпека відеоконференцій та онлайн-нарад

✓ ПОТРІБНО РОБИТИ

- Унікальний пароль для кожної наради
- Зал очікування (Waiting Room) активовано
- Перевірка учасників перед допуском
- Тільки схвалені платформи (Signal, Element/Matrix для держорганів)
- Шифрування E2E обов'язкове для конфіденційних нарад
- Заборона запису без згоди всіх учасників

✗ НЕ ДОПУСКАЄТЬСЯ

- Не публікуйте посилання в публічних чатах
- Не обговорюйте ДСК у незахищених каналах
- Не використовуйте Zoom, Teams для таємних нарад
- Не дозволяйте спільний екран без потреби
- Не ігноруйте невідомих учасників нарад

Аналіз маніпулятивного листа

Поштовий клієнт – Нове повідомлення

Від: **it.support@minfinua-gov.net (підроблений домен!)**

Кому: dept-users@minfin.gov.ua

Тема: **ТЕРМІНОВО: Ваш обліковий запис буде заблоковано через 24 год**

Шановний співробітнику,

Ваш обліковий запис потребує НЕГАЙНОЇ верифікації.
Перейдіть за посиланням протягом 24 годин:

www.minfin-security-update.ru/login

Відділ IT-безпеки

Ознаки маніпуляції

- Підроблений домен відправника
- Штучне відчуття терміновості
- Зовнішнє посилання (.ru домен)
- Вимога перейти за посиланням
- Без персонального звертання
- Вкладення з подвійним розширенням

Ключові висновки та рекомендації

1

Принцип нульової довіри

Zero Trust Architecture – перевіряти кожного користувача та пристрій при кожному запиті, незалежно від локації

2

Культура безпеки

Регулярні тренінги, симуляції фішингу, культура повідомлення про інциденти без покарання

3

Моніторинг 24/7

SOC/CERT з безперервним моніторингом, SIEM-система, автоматичне сповіщення про аномалії

4

Готовність до інцидентів

Актуальний план IRP, регулярні навчання та тест-прогони процедур реагування

5

Управління ризиками

Регулярні тести на проникнення, оцінка вразливостей, Risk Register

Державна служба спеціального зв’язку
та захисту інформації України

ДЕРЖНДІ · 5 ЦЕНТР· 2026

ДЯКУЮ ЗА УВАГУ!

5 Центр ДержНДІ технологій кібербезпеки