ДОРОЖНЯ КАРТА КІБЕРСТІЙКОСТІ

Куди рухатись за максимальним захистом ІКС

Чотири рівні зрілості захисту — від обов'язкового фундаменту до проактивного центру безпеки. Кожна підсистема закриває конкретну вимогу базового профілю безпеки та відповідний захід NIST. Рухайтесь знизу вгору: спочатку — основа, без якої не пройти авторизацію, далі — поглиблення захисту.

ПРОФІЛЬ БЕЗПЕКИ	ПОРЯДОК АВТОРИЗАЦІЇ	СТАНДАРТ
Наказ ДССЗЗІ № 409 · відкрита / конфіденційна	**Постанова КМУ № 712** · від 18.06.2025	**NIST CSF** · SP 800-53

ЗРОСТАННЯ ЗАХИЩЕНОСТІ →

4 ПРОАКТИВНИЙ

Проактивна оборона

ЗРІЛИЙ SOC · ОПЦІЯ

Автоматизація реагування та поведінкова аналітика. Для великих органів із власним центром безпеки.

- **Автоматизація реагування (SOAR)** RS.MA-01 / IR-4
- **Поведінкова аналітика (UEBA)** DE.AE-02
- **Аналітика загроз на базі ШІ** DE.AE-07

3 СИСТЕМНИЙ

Видимість і контроль даних

ПОГЛИБЛЕННЯ · ОПЦІЯ

Централізований збір подій, захист веб-додатків і запобігання витоку інформації.

- **Керування подіями безпеки (SIEM)** DE.CM-01 / AU-6
- **Централізований збір журналів** DE.AE-03 / AU-9
- **Захист веб-додатків (WAF)** PR.IR-01 / SI-10
- **Захист від DDoS-атак** PR.IR-04 / SC-5
- **Запобігання витоку даних (DLP)** PR.DS-01

2 ФОКУСНИЙ

Контроль доступу та вразливостей

ОБОВ'ЯЗКОВО

Хто і що підключається до систем, і де слабкі місця. Обов'язково від 200 користувачів.

- **Контроль дій адміністраторів (PAM)** PR.AA-05 / AC-6
- **Контроль підключення пристроїв (NAC)** PR.AA-06 / AC-3
- **Пошук вразливостей систем** ID.RA-01 / RA-5
- **EDR — виявлення та реагування на хостах** DE.CM-09 / SI-4

1 БАЗОВИЙ

Фундамент захисту

ОБОВ'ЯЗКОВИЙ МІНІМУМ

Без цього рівня система не пройде авторизацію. Основа, на якій тримається все інше.

- **Служба каталогів (AD)** PR.AA-01 / IA-2
- **Міжмережевий екран (пара)** PR.IR-01 / SC-7
- **Багатофакторний вхід (MFA)** PR.AA-03 / IA-2(1)
- **Антивірусний захист (Endpoint Protection)** DE.CM-09 / SI-3
- **Облік активів і оновлення ПЗ** ID.AM-01 / SI-2
- **Резервне копіювання даних** PR.DS-11 / CP-9

◀ НЕЗМІННА ОСНОВА

Під усіма рівнями — відмовостійка платформа (**НСІ-кластер**, ДБЖ, захищена шафа) та **гарантоване зберігання копій і журналів**: дані йдуть на ізольований сервер через апаратний односторонній шлюз, тож при зломі мережі їх неможливо видалити чи змінити.

ПРИНЦИП	ОРІЄНТИР	РЕЗУЛЬТАТ
Глибина, а не точка. Кожен рівень страхує наступний. Захист будується цілісно — від виявлення ризику до відновлення.	**Спочатку фундамент.** Рівні 1–2 — обов'язкові для авторизації. Рівні 3–4 додають зрілість у міру зростання органу.	**Готовність до перевірки.** Доказова відповідність вимогам держави (№ 712) та світовим стандартам NIST.

AMI GROUP Integrator

СИСТЕМНА ІНТЕГРАЦІЯ · КІБЕРЗАХИСТ ІКС

Тел. +38 (044) 394-86-07

E-mail mail@amintegrator.com