Комплексна система захисту інформації

Політики і модель профілів безпеки

Зміст

1. Вступ

На підприємствах (недержавних суб'єктах) у 2026 році КСЗІ (Комплексна Система Захисту Інформації) переходить на модель профілів безпеки і Авторизацію безпеки Систем Захисту (АСЗ) відповідно до Постанови КМУ № 712 від 18 червня 2025 року.

2. Нормативно-правова база (НПА)

- Постанова КМУ № 712 від 18.06.2025 («Порядок розроблення та затвердження профілів безпеки...» та «Порядок авторизації...»).
- Закон України «Про судоустрій і статус суддів» (№ 1402-VIII від 02.06.2016).
- Закон України «Про захист інформації в інформаційно-комунікаційних системах».
- Закон України «Про основні засади забезпечення кібербезпеки України».
- Нормативні документи ТЗІ (НД ТЗІ 3.6-004-21, 3.6-005-21, 3.6-006-24 тощо).

3. Основні типи профілів безпеки

- Базовий профіль — затверджується Адміністрацією Держспецзв'язку (наказом).
- Галузевий профіль — розробляється галузевим органом, погоджується з Держспецзв'язку та затверджується наказом/рішенням відповідного органу.
- Цільовий профіль безпеки (ЦПБ) — індивідуальний для конкретної системи підприємства. Саме на його основі створюється/модернізується КЗЗІ.

4. Формат затвердження та прийняття на підприємстві

Для цільового профілю безпеки на підприємстві (власник/розпорядник системи) затвердження відбувається внутрішнім організаційно-розпорядчим документом:

- Наказом керівника підприємства (директора, генерального директора тощо).
- Або рішенням уповноваженого органу управління (для ТОВ, АТ тощо — протоколом зборів засновників/наглядової ради, якщо це передбачено статутом).

Цільовий профіль розробляється на основі базового (або галузевого, якщо є) з урахуванням:

- Результатів оцінки ризиків.
- Особливостей системи.
- Нормативних документів ТЗІ (НД ТЗІ 3.6-004-21, 3.6-005-21, 3.6-006-24 тощо).

5. Процес (коротко)

1. Обстеження системи та оцінка ризиків.
2. Формування ЦПБ (сукупність заходів захисту).
3. Затвердження внутрішнім наказом керівника підприємства.
4. Документування (політика безпеки інформації тощо).
5. Впровадження заходів, оцінка відповідності.

Цільовий профіль не потребує зовнішнього затвердження Держспецзв'язку для звичайних підприємств (на відміну від базових/галузевих). Він є основою для декларування/авторизації відповідності системи захисту.

6. Структура конструкторської документації

В Україні структура та "шаблони"для цих документів чітко регламентовані державними стандартами (ДСТУ). Оскільки розробляються IT-продукти (месенджер, VPN, АЦСК), слід опиратися на ДСТУ ISO/IEC 15408 (Загальні критерії) та стандарти на конструкторську документацію.

Ось типові структури (шаблони) для кожного з цих документів:

6.1. Завдання з безпеки (Security Target, ST)

Регулюється: ДСТУ ISO/IEC 15408-1 (Додаток B). Це головний документ для конкретного продукту (наприклад, `synrc/chat`), який подається на експертизу.

Типова структура:

1. Вступ до ЗБ (ST Introduction)
    - Ідентифікація Завдання з безпеки та Об'єкта оцінювання (ОО).
    - Огляд ОО (призначення, основні функції).
2. Опис Об'єкта оцінювання (TOE Description)
    - Архітектура, фізичні та логічні межі продукту.

3. Середовище безпеки ОО (TOE Security Environment)
    - Припущення (щодо безпеки середовища, де працює продукт).
    - Загрози (що саме може порушити безпеку).
    - Політики безпеки організації.
4. Цілі безпеки (Security Objectives)
    - Цілі безпеки для самого ОО (продукту).
    - Цілі безпеки для середовища (що має забезпечити ОС або адміністратор).
5. Вимоги безпеки IT (IT Security Requirements)
    - Функціональні вимоги безпеки ОО (SFR) — саме сюди мапляться контролі AC-2, SC-8 тощо з `l2_*.ex`.
    - Вимоги довіри до безпеки ОО (SAR) (наприклад, рівні EAL).
6. Зведена специфікація ОО (TOE Summary Specification)
    - Опис функцій безпеки ОО (як саме продукт реалізує кожну вимогу).
    - Заходи довіри.
7. Обґрунтування (Rationale)
    - Доведення того, що вимоги перекривають загрози, а функції виконують вимоги.

6.2. Профіль захисту (Protection Profile, PP)

Регулюється: ДСТУ ISO/IEC 15408-1 (Додаток А). Структура майже ідентична "Завданню з безпеки але Профіль захисту пишеться не для конкретного продукту, а для класу продуктів (наприклад, "Вимоги до військових месенджерів").

Типова структура:

1. Вступ до ПЗ (PP Introduction)
2. Опис ОО (TOE Description)
3. Середовище безпеки ОО (TOE Security Environment)
4. Цілі безпеки (Security Objectives)
5. Вимоги безпеки IT (IT Security Requirements)
6. Зауваження щодо застосування (Application Notes) — специфічний для ПЗ розділ.
7. Обґрунтування (Rationale) (Тут немає "Зведеної специфікації бо немає конкретної реалізації продукту).

6.3. Технічні умови (ТУ) на програмний продукт

Регулюється: ГОСТ 2.114-95, СОУ-Н МПП 01.120-090:2005 (для ПЗ) або ДСТУ-Н 1.3:2015. Це базовий технічний документ підприємства, за яким випускається продукт.

Типова структура ТУ:

1. Сфера застосування (Призначення продукту).
2. Нормативні посилання (ДСТУ, НД ТЗІ, якими ви керувалися).
3. Технічні вимоги:

- Основні параметри та характеристики (функціонал).
- Вимоги до надійності.
- Вимоги до інформаційної безпеки (тут зазвичай іде посилання на ваше "Завдання з безпеки або коротко перелічуються ключові вимоги).
- Вимоги до програмної та апаратної сумісності (системні вимоги).
- Комплектність.
- Маркування та пакування (якщо є фізичні носії чи коробкові версії).

4. Вимоги безпеки (Охорона праці для адміністраторів/користувачів — стандартний розділ).
5. Правила приймання (Порядок проведення випробувань: приймально-здавальних, періодичних).
6. Методи контролю (випробувань) (Як саме тестується продукт і перевіряється безпека).
7. Транспортування та зберігання.
8. Вказівки щодо експлуатації.
9. Гарантії розробника (виробника).

6.4. Галузевий профіль безпеки (для державних органів та сфер)

Регулюється: НД ТЗІ 3.6-006-24. Розробляється для певної сфери (наприклад, енергетика, банки, судова влада) на основі базового профілю.

Типова структура:

1. Вступ:
   - Мета та сфера дії профілю.
   - Посилання на базовий профіль безпеки.
2. Опис галузевих особливостей:
   - Специфіка обробки інформації в галузі.
   - Специфічні загрози та ризики.
   - Визначення зацікавлених сторін.
3. Перелік заходів захисту:
   - Заходи, вибрані з базового профілю.
   - Додаткові (посилені) заходи, необхідні для галузі.
4. Налаштування заходів (Tailoring):
   - Значення параметрів заходів захисту, специфічні для галузі.
   - Вказівки щодо впровадження.

6.5. Цільовий профіль безпеки (для конкретної державної інформаційної системи)

Регулюється: НД ТЗІ 3.6-006-24. Розробляється на основі галузевого (або базового) профілю для конкретної системи, яка створюється та проходить експертизу в держсекторі.

Типова структура:

1. Загальні відомості:
    - Призначення та межі інформаційної системи (ІС).
    - Характеристика оброблюваної інформації та критичності процесів.
2. Оцінка ризиків:
    - Результати оцінки ризиків ІС.
    - Обґрунтування необхідності специфічних заходів.
3. Специфікація заходів захисту:
    - Перелік вибраних заходів захисту (включно зі значеннями всіх параметрів, призначених для цієї конкретної ІС).
    - Обґрунтування вибраних заходів (tailoring rationale).
4. Організаційні та технічні вимоги:
    - Вимоги до середовища функціонування.
    - Вимоги до персоналу.

Для продуктів створюється ТУ. В розділі "3. Технічні вимоги"додається пункт "Вимоги щодо технічного захисту інформації де вказується: "Програмний комплекс має відповідати вимогам Завдання з безпеки ЗБ.12345678.001". А вже саме Завдання з безпеки генерується з `.ex` файлів, де детально розписуються всі контроли (AC, SC, AU тощо), матриці доступу і криптографія.

7. Завдання з безпеки для IT-продуктів

Нижче наведено структуру Завдань з безпеки (Security Targets) для розроблених продуктів, згідно з галузевими профілями L2.

7.1. Завдання з безпеки для ERP/1 Комунікатор

Призначення: Забезпечення конфіденційності, цілісності повідомлень та управління сесіями в месенджері з підтримкою E2EE, ефемерних повідомлень та захисту пуш-повідомлень.

Модульна структура профілю:

- synrc/chat (Ядро месенджера): Наскрізне шифрування (SC-8), шифрування історії на пристрої (SC-28), керування паралельними сесіями (AC-10), ефемерні/зникаючі повідомлення (MP-6), біометрична автентифікація (IA-5) та захист мобільних пристроїв (AC-19).
- synrc/ldap (Служба каталогів): Ідентифікація користувачів (IA-2, IA-4), керування доступом до каталогу (AC-2, AC-3, AC-6) та реєстрація подій (AU-2).

- synrc/ns (Сервер імен): Безпечне розрізнення імен DNSSEC (SC-20, SC-21, SC-22), захист від DoS (SC-5) та захист меж мережі (SC-7).
- synrc/ca (PKI інфраструктура): Інфраструктура відкритих ключів (SC-17, SC-12), цифрові підписи та мітки часу TSP (AU-10), апаратне виконання в HSM (SC-49, SC-51, IA-7).
- synrc/kvs (Сховище Key-Value): Захист інформації у стані спокою (SC-28), резервне копіювання (CP-9) та аудит транзакцій (AU-2).

7.2. Завдання з безпеки для ERP/1 Документи

Призначення: Забезпечення конфіденційності, цілісності та гарантованої доставки повідомлень (MHS X.420 / STANAG 4406) з підтримкою грифування, S/MIME та неспростовності.

Функціональні вимоги та компоненти:

- Захист передачі та E2EE: Конфіденційність передачі через CMS / S/MIME (SC-8) та шифрування листів у стані спокою (SC-28).
- Грифування та атрибути безпеки: Маркування суб'єктів/об'єктів (AC-16) та пониження грифу таємності (MP-8).
- Неспростовність та ЕЦП: Докази походження та доставки повідомлень (AU-10).
- Сувора автентифікація: Підтримка смарт-карток та PKI Credentials (IA-2, IA-5).
- Механізм контролю доступу (ABAC): Reference Monitor (AC-25) та перевірка політик доступу (AC-3).
- Бізнес-процеси та маршрутизація (BPMN): Управління потоками за BPMN (AC-4), обмеження зміни схем (CM-5) та логування транзицій станів (AU-12).

7.3. Завдання з безпеки для ERP/1 VPN CA PKI

Призначення: Забезпечення безпеки VPN-продуктів (tunctl) та комплексної інфраструктури відкритого ключа (CA, OCSP, TSP, LDAP).

Функціональні вимоги та компоненти:

- VPN та мережевий доступ: Шифрування тунелів, можливість примусового розриву (AC-17), заборона Split Tunneling (SC-7), розрив неактивних сесій (SC-10) та захист після встановлення (SC-23).
- Інфраструктура PKI: Випуск/відкликання сертифікатів (SC-17), протоколи CMP/EST (SC-12), автентифікація mTLS (IA-5), використання HSM для CA/OCSP/TSP (SC-49, SC-51, IA-7).
- Каталог та Ідентифікація: Підтримка MFA, кваліфікованих сертифікатів та EUDI Wallet (IA-2), управління LDAP (IA-4, AC-2, AC-3).
- Криптографічний захист: Захист даних в русі (SC-8) та баз даних каталогів у стані спокою (SC-28).

8. Ієрархія профілів безпеки

Відповідно до Закону України «Про судоустрій і статус суддів», стаття 17 «Система судоустрою»:

1. Судоустрій будується за принципами територіальності, спеціалізації та інстанційності.
2. Найвищим судом у системі судоустрою є Верховний Суд.
3. Систему судоустрою складають: 1) місцеві суди; 2) апеляційні суди; 3) Верховний Суд.

На базі цього визначено таксономію профілів безпеки за відповідними OID:

- 1.2.804.3.1.2.1 — Базовий профіль безпеки (L1)
- 1.2.804.3.1.2.2 — Галузевий профіль безпеки (L2)
- 1.2.804.3.1.2.3 — Цільовий профіль безпеки вищих судів (L3)
  - 1.2.804.3.1.2.3.1 — Велика Палата Верховного Суду
  - 1.2.804.3.1.2.3.2 — Касаційний адміністративний суд
  - 1.2.804.3.1.2.3.3 — Касаційний господарський суд
  - 1.2.804.3.1.2.3.4 — Касаційний кримінальний суд
  - 1.2.804.3.1.2.3.5 — Касаційний цивільний суд
- 1.2.804.3.1.2.4 — Цільовий профіль безпеки вищих спеціалізованих судів (L3)
  - 1.2.804.3.1.2.4.1 — Вищий суд з питань інтелектуальної власності
  - 1.2.804.3.1.2.4.2 — Вищий антикорупційний суд
  - 1.2.804.3.1.2.4.3 — Спеціалізований окружний адміністративний суд
  - 1.2.804.3.1.2.4.4 — Спеціалізований апеляційний адміністративний суд
- 1.2.804.3.1.2.5 — Цільовий профіль судів (L3)
  - 1.2.804.3.1.2.5.1 — Цільовий профіль безпеки місцевих судів (L4)
  - 1.2.804.3.1.2.5.2 — Цільовий профіль безпек апеляційних судів (L4)
- 1.2.804.3.1.2.6 — Цільовий профіль безпеки органів та установ у системі правосуддя (L3)
  - 1.2.804.3.1.2.6.1 — ДСА (L4)
  - 1.2.804.3.1.2.6.2 — ТУ ДСА, допоміжні установи (L4)
  - 1.2.804.3.1.2.6.3 — Рада суддів України (L4)
  - 1.2.804.3.1.2.6.4 — ВРП (L4)
  - 1.2.804.3.1.2.6.5 — ВККСУ (L4)
  - 1.2.804.3.1.2.6.6 — Національна школа суддів України (L4)
  - 1.2.804.3.1.2.6.7 — ГРД та ГРМЕ (L4)
  - 1.2.804.3.1.2.6.8 — Служба судової охорони (L4)

Якщо у вас державна система, об'єкт КІІ чи специфічна галузь — порядок може відрізнятися (погодження/затвердження з Держспецзв'язку або галузевим органом). Рекомендую звернутися до відділу ТЗІ або спеціалізованої організації для конкретної системи.

9. Галузевий профіль безпеки (L2)

Цей профіль розширює базовий (L1) додатковими вимогами, які адаптовано для специфіки сучасних мобільних пристроїв, багатофакторної автентифікації та використання сертифікованих апаратних засобів криптографічного захисту (КЗІ).

Мотивація вибору додаткових заходів захисту:

1. Сучасні мобільні екосистеми (Apple iPhone, Face ID, Passkeys):
   - `IA-5(12)`, `IA-5(17)`: Забезпечення надійності біометрики та захист від спуфінгу (увага до екрана Face ID).
   - `IA-2(12)`: Підтримка PIV Credentials та технології Passkeys (FIDO2) для безпарольного доступу.
   - `AC-7(2)`, `AC-19(4)`: Відповідність політикам MDM (обмеження для засекреченої інформації, стирання пристрою після невдалих спроб входу).
2. Апаратні криптографічні модулі (ІІТ Сайфер, Автор ПК КЗІ, HSM):
   - `IA-5(11)`, `IA-5(15)`: Підтримка апаратних токенів та використання виключно сертифікованих уповноваженим органом продуктів.
   - `IA-7`: Строга автентифікація самого криптографічного модуля.
   - `SC-49`, `SC-51`: Примусове апаратне забезпечення виконання та апаратний захист (запобігання витягуванню ключів).
   - `SC-12`, `SC-17`, `SC-28(1)`: Криптографічне управління ключами, PKI-сертифікати та шифрування даних у стані спокою.
3. Судді (робота на ноутбуках):
   - `AC-19(1)`, `AC-19(2)`: Контроль доступу для портативних та персональних пристроїв зберігання даних.
   - `MP-6`: Знищення інформації на носіях (підтримка Remote Wipe / Activation Lock).
4. Відеоконференції:
   - `SC-44`: Екрановані камери (захист від несанкціонованого відеоспостереження).
   - `SC-15` (успадковано з базового L1): Захист спільних обчислювальних пристроїв та засобів ВКЗ.
5. Електронний документообіг:
   - `AU-10`, `AU-10(5)`: Неспростовність та використання цифрових підписів для гарантії авторства документів.
   - `SI-7`: Забезпечення цілісності інформації та програмного забезпечення.
6. Службова та таємна інформація (Матеріали справ):
   - `AC-15`, `AC-16`: Автоматизоване маркування документів та управління атрибутами безпеки (Classification & Labeling).
   - `MP-8(4)`: Безпечне зниження категорії безпеки для таємної інформації (Downgrading).
   - `PE-22`: Маркування компонентів та обладнання, де обробляються засекречені дані.

10. Класи (сімейства) заходів захисту

Усі заходи захисту інформації в КЗЗІ згруповані у відповідні класи (сімейства), які охоплюють різні аспекти інформаційної безпеки:

- AC (Управління доступом): Цей клас зосереджується на обмеженні доступу до інформаційних систем, ресурсів та функцій лише для авторизованих користувачів, програм і пристроїв.
- AT (Обізнаність та навчання): Цей клас спрямований на забезпечення належного рівня знань персоналу щодо загроз інформаційній безпеці та їхніх обов'язків у цій сфері.
- AU (Аудит та підзвітність): Цей клас забезпечує можливість відстеження дій у системі, генерування, захист та аналіз записів аудиту для виявлення порушень політики безпеки.
- CA (Оцінювання, авторизація та моніторинг): Цей клас регламентує процеси перевірки ефективності заходів захисту, авторизації систем та їх безперервного моніторингу.
- CM (Управління конфігурацією): Цей клас гарантує створення та підтримання базових налаштувань системи, а також строгий контроль за змінами в апаратному та програмному забезпеченні.
- CP (Планування безперервної роботи): Цей клас описує заходи для відновлення функціонування інформаційної системи та забезпечення її безперебійної роботи у разі надзвичайних ситуацій.
- IA (Ідентифікація та автентифікація): Цей клас відповідає за однозначне розпізнавання користувачів або пристроїв та підтвердження їхньої справжності перед наданням доступу до системи.
- IR (Реагування на інциденти): Цей клас визначає процедури виявлення, аналізу, локалізації та усунення наслідків інцидентів інформаційної безпеки.
- MA (Технічне обслуговування): Цей клас регулює процеси планового та позапланового технічного обслуговування компонентів системи для запобігання збоям.
- MP (Захист носіїв інформації): Цей клас спрямований на безпечне зберігання, транспортування, використання та знищення як цифрових, так і паперових носіїв інформації.
- PE (Фізичний захист та захист навколишнього середовища): Цей клас охоплює заходи контролю фізичного доступу до об'єктів організації та захисту обладнання від загроз навколишнього середовища.
- PL (Планування): Цей клас регламентує розробку, документування та регулярне оновлення планів захисту інформації, архітектури безпеки та приватності.
- PS (Безпека персоналу): Цей клас встановлює вимоги до перевірки, надання повноважень та звільнення персоналу з метою мінімізації ризиків інсайдерських загроз.
- RA (Оцінка ризиків): Цей клас забезпечує систематичний підхід до виявлення, аналізу та реагування на ризики, пов'язані з обробкою інформації та функціонуванням системи.
- SA (Придбання систем та послуг): Цей клас зосереджується на інтеграції вимог безпеки на всіх етапах життєвого циклу розробки та закупівлі IT-продуктів чи послуг.
- SC (Захист систем та комунікацій): Цей клас охоплює механізми захисту інформації під час її передачі мережами зв'язку, криптографічний захист та ізоляцію критичних компонентів.
- SI (Цілісність системи та інформації): Цей клас спрямований на захист системи від шкідливого коду, виявлення вразливостей та запобігання несанкціонованим змінам інформації.

- SR (Управління ризиками в ланцюгу постачання): Цей клас встановлює вимоги для виявлення та мінімізації загроз, що виникають через зовнішніх постачальників продуктів та послуг.
- PM (Управління програмами): Цей клас визначає загальноорганізаційні заходи для ефективного управління програмами інформаційної безпеки та приватності на рівні всього підприємства.
- PT (Обробка персональних даних та прозорість): Цей клас фокусується на дотриманні законодавства щодо захисту персональних даних, отриманні згоди та забезпеченні прав суб'єктів даних.

11. Матриця доступу та ролей (ABAC/RBAC)

11.1. Системні та людські ролі

- R-SYS: Системний процес (Machine-to-Machine) — Автоматичні сервіси (OCSP-респондер, CRL-генератор).
  Контролі: SC, IA
- R-OPR: Оператор реєстрації — Права на генерацію запитів на сертифікати, перевірку документів підписників.
  Контролі: AC, IA
- R-ADM: Адміністратор безпеки — Повний контроль над конфігурацією систем захисту, але без доступу до бізнес-даних.
  Контролі: AC, IA, AU
- R-AUD: Аудитор — Право на читання журналів подій та конфігурацій (Read-Only).
  Контролі: AU, AC

11.2. Політики управління доступом

- POL-01: Багатофакторна автентифікація (MFA) обов'язкова для R-ADM.
- POL-02: R-OPR може створювати запити лише в межах своєї локації (Location-based ABAC).
- POL-03: Доступ до систем керування ключами вимагає 'Правила двох осіб' (Dual Control / Split Knowledge).

12. Класифікація інформаційних масивів

- D-INT: Службова інформація — Внутрішні накази, конфігураційні файли, журнали аудиту.
  Вплив: Conf: medium, Int: high, Avail: high
  Контролі: AC, AU, CM
- D-PUB: Публічна інформація — Дані, розкриття яких не несе ризиків (публічні сертифікати, CRL, політики ЦСК).
  Вплив: Conf: low, Int: high, Avail: high
  Контролі: SI, CP
- D-BKP: Резервні копії (Backups) — Снапшоти баз даних, образи ВМ, архіви судових документів.
  Вплив: Conf: high, Int: high, Avail: high
  Контролі: CP, MP, PE, SC
- D-CRT: Електронні судові справи — Матеріали судових проваджень, ухвали, рішення, докази (в т.ч. з обмеженим доступом).
  Вплив: Conf: high, Int: high, Avail: high
  Контролі: AC, SC, SI, CP
- D-PII: Персональні дані — Паспортні дані, РНОКПП, адреси підписників.
  Вплив: Conf: high, Int: high, Avail: medium
  Контролі: SC, AC, PE, AU
- D-KEY: Ключова інформація — Особисті ключі ЦСК, сесійні ключі шифрування, паролі адміністраторів.
  Вплив: Conf: high, Int: high, Avail: high
  Контролі: SC, PE, MP, IA

13. Апаратне забезпечення (HW Inventory)

13.1. Network

- HW-NET-01: Маршрутизатори та комутатори ядра
  Контролі: SC, CM, PE
- HW-NET-02: Міжмережеві екрани (Firewalls, IDS/IPS)
  Контролі: SC, AU, CM

13.2. Endpoints

- HW-END-01: Робочі станції операторів / адміністраторів
  Контролі: PE, AC, SI
- HW-END-02: Мобільні пристрої
  Контролі: AC, SC, MP

13.3. Kzi

- HW-KZI-01: Апаратні криптомодулі (HSM / Гряда)
  Контролі: PE, MP, SC, IA
- HW-KZI-02: Захищені носії ключової інформації (e-Токени, Смарт-карти)
  Контролі: MP, PE, IA

13.4. Servers

- HW-SRV-01: Фізичні сервери (On-Premise)
  Контролі: PE, CP, CM
- HW-SRV-02: Віртуальні машини / Гіпервізори
  Контролі: SC, CM, SI

13.5. Storage

- HW-STG-01: Системи зберігання даних (СЗД, SAN, NAS)
  Контролі: PE, MP, CP
- HW-STG-02: Стрічкові бібліотеки (Tape Libraries) для офлайн бекапів
  Контролі: PE, MP

14. Мережева топології та зонування

- Z-INT: Внутрішня мережа — Сервери баз даних, внутрішні портали, робочі станції операторів.
  Контролі: SC, AC, PE
- Z-AIR: Ізольоване середовище (Air-gapped) — Офлайн-Вузол ЦСК (Кореневий ЦСК), фізично відключений від мереж передачі даних.
  Контролі: PE, MP, AC, CM
- Z-DMZ: Демілітаризована зона (DMZ) — Сервери, доступні з інтернету (Web, OCSP, CRL endpoints).
  Контролі: SC, AU, AC
- Z-MGT: Мережа управління (OOB Management) — Виділений VLAN для адміністрування (SSH, IPMI) без прямого доступу з інших мереж.
  Контролі: IA, AC, SC, AU

15. Критичність бізнес-процесів

- P-AUDIT: Логування та моніторинг — Запис подій безпеки у централізоване сховище (SIEM).
  Критичність: high, RTO: 24 год, RPO: 0 год
  Контролі: AU, CP
- P-BKP: Резервне копіювання та відновлення — Процес створення, верифікації та безпечного зберігання бекапів.
  Критичність: critical, RTO: 24 год, RPO: 0 год
  Контролі: CP, MP, SI
- P-ISSUE: Видача сертифікатів — Процес обробки CSR та формування підписаного сертифіката.
  Критичність: high, RTO: 4 год, RPO: 1 год
  Контролі: CP, SI
- P-DOC: Електронний документообіг (Судові справи) — Обробка, зберігання та обіг електронних судових документів, ухвал, рішень.
  Критичність: high, RTO: 8 год, RPO: 2 год
  Контролі: SI, AC, CP, AU
- P-OCSP: Формування OCSP-відповідей — Надання інформації про статус сертифіката в реальному часі.
  Критичність: critical, RTO: 0 год, RPO: 0 год
  Контролі: CP, SC
- P-ROOT: Церемонія генерації кореневого ключа — Рідкісний, але гіперкритичний офлайн-процес.
  Критичність: critical, RTO: 72 год, RPO: 0 год
  Контролі: PE, AC, PS, AU

16. Програмне забезпечення (Software Inventory)

16.1. Os

- SYS-OS-01: Серверні ОС (Linux, Windows Server)
  Контролі: CM, SI, AC
- SYS-OS-02: Клієнтські ОС (Windows 11)
  Контролі: CM, SI, AC

16.2. App

- SYS-APP-01: Програмні комплекси ЦСК (Сайфер, ІІТ)
  Контролі: SI, SC, AU, CP
- SYS-APP-02: Системи моніторингу та логування (SIEM, Zabbix)
  Контролі: AU, IR

16.3. Infrastructure

- SYS-INF-01: Системи резервного копіювання (Veeam, Bacula)
  Контролі: CP, CM, SC, AU

16.4. Db

- SYS-DB-01: Реляційні СУБД (PostgreSQL, Oracle)
  Контролі: SC, AC, AU, CP
- SYS-DB-02: NoSQL та кеші (Redis, MongoDB)
  Контролі: SC, AC, AU

16.5. Middleware

- SYS-MW-01: Веб-сервери та балансувальники (Nginx, HAProxy)
  Контролі: SC, CM, AU
- SYS-MW-02: Сервіси каталогів (Active Directory, FreeIPA)
  Контролі: IA, AC, SC

17. Таксономія та карта ризиків

17.1. Операційні системи

17.1.1 Windows

- R-OS-W-01: Вразливості Active Directory (Advanced) — Атаки Kerberoasting, AS-REP Roasting, Pass-the-Hash, Golden/Silver Ticket, DCSync, DCShadow.
  Контролі: AC, IA, SC
- R-OS-W-02: Зловживання WMI та PowerShell — Використання Windows Management Instrumentation та Fileless-методів для виконання коду та персистентності.
  Контролі: SI, SC, CM
- R-OS-W-03: Вразливості на рівні ядра (Ring 0) — Експлуатація вразливостей сторонніх драйверів (BYOVD) для обходу EDR та PatchGuard.
  Контролі: SI, CM
- R-OS-W-04: Маніпуляція маркерами доступу — Token Stealing, маніпуляція привілеями (SeDebugPrivilege, SeImpersonatePrivilege) для ескалації.
  Контролі: AC, AU
- R-OS-W-05: Некоректні дозволи NTFS / Share — Отримання доступу до файлів через помилки в налаштуваннях ACL або залишкові права (Orphaned SIDs).
  Контролі: AC, CM

17.1.2 Linux

- R-OS-L-01: Підвищення привілеїв (Kernel & SUID) — Експлуатація локальних вразливостей ядра (Dirty COW, Dirty Pipe), SUID-бінарників та Capabilities.
  Контролі: AC, SI
- R-OS-L-02: Втеча з контейнерів (Container Escape) — Прорив ізоляції Docker/Kubernetes через зловживання просторами імен (Namespaces), cgroups, або сокетом Docker.
  Контролі: SC, CM
- R-OS-L-03: Зловживання eBPF — Використання Extended Berkeley Packet Filter для прихованого моніторингу та маніпуляції системними викликами.
  Контролі: AU, SI
- R-OS-L-04: Ін'єкції динамічних бібліотек — Перехоплення викликів через LD_PRELOAD або маніпуляція RPATH/RUNPATH для виконання шкідливого коду.
  Контролі: SI, CM
- R-OS-L-05: Вразливості PAM — Некоректна конфігурація Pluggable Authentication Modules, що дозволяє обхід автентифікації.
  Контролі: IA, AC

17.2. Інфраструктура

- R-INF-01: Експлуатація Baseboard Management Controller (BMC) — Компрометація інтерфейсів IPMI, iDRAC, iLO для повного контролю над сервером поза межами ОС.
  Контролі: AC, SC
- R-INF-02: Вразливості Firmware / UEFI Bootkits — Впровадження шкідливого коду (Bootkits) на рівні материнської плати або контролерів для персистенції.
  Контролі: SI, SA

- R-INF-03: Атаки на мікроархітектуру CPU — Спекулятивне виконання (Spectre, Meltdown) та маніпуляції з кешем для екстракції криптоключів з інших ВМ.
  Контролі: SI, SC
- R-INF-04: Атаки Cold Boot & Rowhammer — Фізичний зріз пам'яті після перезавантаження (Cold Boot) або зміна бітів пам'яті сусідніх комірок (Rowhammer).
  Контролі: PE, SI
- R-INF-05: Відмова дискових масивів (SAN/NAS) — Синхронна відмова множини дисків (Split-brain в кластерах), корупція метаданих файлових систем.
  Контролі: CP, SI
- R-INF-06: Електромагнітне випромінювання (TEMPEST) — Перехоплення даних шляхом аналізу побічних електромагнітних випромінювань від моніторів або кабелів.
  Контролі: PE, SC
- R-INF-07: Відмова інженерних систем життєзабезпечення — Синхронна відмова ДЖБ (UPS), дизель-генераторів, систем чиллерів або установок газового пожежогасіння.
  Контролі: PE, CP

17.3. Мережа

- R-NET-01: BGP Hijacking & Route Leaks — Підміна анонсів автономних систем (AS) для перехоплення або Blackholing трафіку.
  Контролі: SC, SI
- R-NET-02: Атаки на протоколи 2-го рівня (L2) — VLAN Hopping, ARP Spoofing, MAC Flooding, атаки на STP (Spanning Tree Protocol) для перехоплення трафіку в LAN.
  Контролі: SC, AC
- R-NET-03: Вразливості IPSec / VPN — Атаки на узгодження IKE, downgrade атак на алгоритми шифрування, витік IKE PSK (Pre-Shared Keys).
  Контролі: SC, IA
- R-NET-04: Мережеве виснаження ресурсів — Складні DDoS атаки рівня додатків (Slowloris), TCP SYN Flood, атаки ампліфікації через DNS, NTP, Memcached.
  Контролі: SC, IR
- R-NET-05: Компрометація Wi-Fi інфраструктури — Атаки KRACK, PMKID ексфільтрація (WPA2/WPA3), Evil Twin (підробні точки доступу).
  Контролі: SC, IA
- R-NET-06: Вразливості протоколу DNSSEC — Підробка відповідей DNS (DNS Spoofing), обхід валідації DNSSEC через помилки конфігурації зон.
  Контролі: SC, SI
- R-NET-07: Відкриті інтерфейси управління — Експлуатація вразливостей в SNMPv1/v2, Telnet, неавтентифікованих REST API на граничному обладнанні.
  Контролі: CM, AC, SC

17.4. Персонал

- R-PER-01: Spear Phishing & Whaling — Цільовий фішинг на ключових осіб (адміністраторів ЦСК) з використанням висококонтекстуальних повідомлень.
  Контролі: AT, IR, SI
- R-PER-02: Watering Hole Attacks — Компрометація профільних веб-ресурсів, які часто відвідує цільова аудиторія, для зараження їх робочих станцій.
  Контролі: SI, AT

- R-PER-03: Інсайдерський саботаж та ексфільтрація — Свідома шкода, логічні бомби, крадіжка комерційної таємниці або приватних ключів авторизованими співробітниками.
  Контролі: PS, AU, AC
- R-PER-04: Зловживання когнітивними упередженнями — Методи претекстінгу (Pretexting), Baiting та Tailgating для отримання фізичного доступу до чистих зон (Clean Rooms).
  Контролі: AT, PE, PS
- R-PER-05: Компрометація облікових даних (Credential Stuffing) — Використання словників та викрадених баз паролів, експлуатація явища повторного використання паролів.
  Контролі: IA, AT

17.5. Синхронізація

- R-SYNC-01: Стан гонитви (Race Condition) — Експлуатація неодночасності доступу до спільних ресурсів, що дозволяє несанкціоновану зміну стану або обхід перевірок.
  Контролі: SI, SA
- R-SYNC-02: Time-of-Check to Time-of-Use (TOCTOU) — Маніпуляція даними (наприклад, файловими посиланнями) між моментом їх перевірки та фактичним використанням системою.
  Контролі: SI, AC
- R-SYNC-03: Десинхронізація часу (NTP Spoofing) — Підміна відповідей NTP для зсуву системного часу, що призводить до валідації прострочених сертифікатів або відмови автентифікації.
  Контролі: SC, AU, SI
- R-SYNC-04: Split-Brain у кластерах — Втрата зв'язку між вузлами кластера з наступною незалежною модифікацією даних (порушення консистентності баз даних).
  Контролі: CP, SI
- R-SYNC-05: Затримки реплікації (Replication Lag) — Експлуатація часового вікна доступу до застарілих даних на Read-репліках СУБД перед їх остаточним оновленням.
  Контролі: SI, SC

17.6. Криптографія та КЗІ

17.6.1 ІІТ

- R-KZI-IIT-01: Компрометація ПАК «Гряда» — Фізичний або логічний доступ до мережевого шифратора або криптомодуля.
  Контролі: PE, SC, AC
- R-KZI-IIT-02: Екстракція ключів з НКІ (е-Токен) — Спроби апаратного зчитування закритого ключа за допомогою мікроскопів або хімічного травлення.
  Контролі: PE, SC
- R-KZI-IIT-03: Вразливості ASN.1 парсерів — Переповнення буфера або DoS при обробці специфічних або зловмисних структур X.509 та CMS інфраструктурою ЦСК.
  Контролі: SI, SA

17.6.2 Cipher

- R-KZI-CIP-01: Вразливості криптобібліотек (ДСТУ) — Помилки при програмній реалізації алгоритмів (Калина, Купина), можливість атак типу Padding Oracle.
  Контролі: SA, SI

- R-KZI-CIP-02: Недостатня ентропія ГВЧ — Генерація передбачуваних ключів через проблеми з апаратним або програмним генератором псевдовипадкових чисел (PRNG).
  Контролі: SC
- R-KZI-CIP-03: Втрата або перехоплення PIN-кодів — Витік аутентифікаційних параметрів адміністраторів HSM через кейлогери або плече-серфінг.
  Контролі: IA, AT, PE

17.6.3 Author

- R-KZI-AUT-01: Фізична деструкція носіїв «Автор» — Виведення з ладу захищених смарт-карт (CryptoCard) через електростатичні розряди або механічне пошкодження.
  Контролі: PE, MP
- R-KZI-AUT-02: Вразливості CCID драйверів — Експлуатація драйверів токенів для ескалації привілеїв у хост-операційній системі.
  Контролі: SI, CM
- R-KZI-AUT-03: Підміна сесій PKCS#11 — Атаки посередника (Man-in-the-Middle) на інтерфейс між програмним забезпеченням ЦСК та модулем HSM.
  Контролі: SC, SI

17.6.4 Загальні

- R-CRY-01: Пост-квантові загрози (SNDL) — Store Now, Decrypt Later атаки на асиметричну криптографію з огляду на розвиток квантових обчислень (алгоритм Шора).
  Контролі: SC, RA, SA
- R-CRY-02: Атаки сторонніми каналами (Side-Channel) — Диференціальний аналіз енергоспоживання (DPA), таймінг-атаки, електромагнітні випромінювання на процесі шифрування.
  Контролі: SC, PE, SA
- R-CRY-03: Атаки внесення помилок (Fault Injection) — Апаратне внесення збоїв (Glitching, Voltage Drop) для пропуску інструкцій автентифікації або перевірки підпису.
  Контролі: PE, SI, SC