SOFTICO | HOLM SECURITY

гайд для фінансових установ

Управління вразливостями у фінансових установах: практична модель з урахуванням вимог НБУ

Практична модель для фінансових установ: від реєстру активів до підтвердженого усунення та звітності.

9 кроків

Від інвентаризації активів до управлінської звітності

Ризик-орієнтований підхід

Пріоритезація за реальним ризиком, а не лише за CVSS (Common Vulnerability Scoring System)

Підтвердження

Що зберігати як підтвердження роботи процесу

Для кого

Банки, страхові компанії, кредитні спілки, фінансові компанії, ломбарди та команди, які будують або вдосконалюють процес управління вразливостями.

Матеріал має інформаційний характер і не є офіційним роз'ясненням НБУ, юридичною консультацією, аудитом або підтвердженням відповідності.

Як користуватися цим гайдом?

Мета — не просто знайти вразливості, а побудувати повторюваний процес: знати активи, оцінювати ризик, виправляти, перевіряти результат і мати докази.

1 Вимога / очікування

Що має бути організовано на рівні процесу.

2 Практична реалізація

Що команда робить технічно й організаційно.

3 Підтвердження

Які документи, звіти або записи варто мати.

Важливо

Точний перелік обов'язкових вимог залежить від типу установи та нормативних актів, що застосовуються саме до неї. Гайд показує практичну модель управління вразливостями, а не замінює юридичний аналіз.

Повний цикл управління вразливостями

Виявлення → Сканування → Оцінка → Пріоритезація →
Усунення → Перевірка → Звітність → Повторення

Ключова ідея: одноразове сканування не дорівнює управлінню вразливостями. Цінність з'являється тоді, коли цикл працює постійно і його можна підтвердити даними.

1. АКТУАЛЬНИЙ РЕЄСТР АКТИВІВ

Не можна захистити те, про існування чого команда безпеки не знає.

Що має бути в реєстрі

- сервери та робочі станції
- мережеве обладнання та зовнішні IP
- вебзастосунки, API та домени
- хмарні ресурси і бази даних
- операційні системи та програмне забезпечення
- системи, що підтримують критичні бізнес-процеси

Що передбачає НБУ

Для небанківських фінансових установ передбачена регулярна актуалізація переліку програмних та апаратних засобів. Для управління вразливостями цього недостатньо робити формально раз на рік, інфраструктура змінюється швидше.

Практичний результат

Для кожного активу має бути зрозуміло:

Що це → **Де знаходиться** → **Хто власник** → **Бізнес-функція** → **Критичність**

Що варто мати як підтвердження

- актуальний реєстр активів
- дата останньої актуалізації
- власник кожного критичного активу
- класифікація за критичністю

2. РЕГУЛЯРНЕ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

Сканування має охоплювати не лише сервери, а всю релевантну поверхню атаки.

Об’єкт	Що шукаємо
Мережа	Відкриті порти, небезпечні служби, конфігурації
ОС та ПЗ	Застарілі версії, відсутні оновлення безпеки
Вебзастосунки	SQLi, XSS, помилки автентифікації та конфігурації
API	Помилки контролю доступу й авторизації
Хмара	Відкриті ресурси, помилки доступу, політики безпеки

Коли запускати перевірки

- регулярно за графіком
- після появи критичної CVE
- після значних змін інфраструктури
- після запуску нового сервісу або міграції
- після оновлення критичних компонентів
- після кіберінциденту

Що варто мати як підтвердження

- політика або процедура сканування
- графік перевірок
- історія сканувань
- покриття активів

3–4. ОЦІНКА РЕАЛЬНОГО РИЗИКУ ТА ПРІОРИТЕЗАЦІЯ

CVSS (Common Vulnerability Scoring System) показує технічну серйозність, але не весь бізнес-ризик.

Що враховувати

Технічна критичність
CVSS, тип вразливості, потенційний вплив

Експлуатованість
Чи є експлойт, чи фіксується активна експлуатація

Зовнішня доступність
Внутрішній актив чи доступний з інтернету

Критичність активу
Яку бізнес-функцію підтримує система

Захисні заходи
WAF, EDR, MFA, сегментація та інші компенсуючі заходи

Вплив на бізнес
Витік даних, простій, компрометація облікових записів

Проста модель
Ризик = технічна критичність × експлуатованість × зовнішня доступність × критичність активу

Приклад: однаковий CVSS ≠ однаковий пріоритет

CVSS 9.8 — тестовий сервер
Ізольований, не доступний з Інтернету, низька бізнес-критичність. Висока технічна серйозність, але нижчий реальний пріоритет.

CVSS 9.8 — критична система
Доступна з Інтернету, пов’язана з критичним процесом, існує експлойт. Першочергове усунення.

Завдання команди інформаційної безпеки не просто сказати «у нас 742 вразливості», а показати, які з них створюють критичний ризик і чому.

5–6. SLA ТА КОНТРОЛЬОВАНЕ УСУНЕННЯ

Приклад внутрішньої SLA-матриці

Рівень	Приклад строку	Примітка
Критичний	24–72 години	Першочергове усунення
Високий	7–14 днів	Найближче вікно усунення
Середній	до 30 днів	Планове усунення
Низький	Плановий цикл	Залежно від ризику

Важливо

Це приклад внутрішніх строків, а не універсальні нормативні строки НБУ. Конкретні SLA визначає сама організація з урахуванням ризику, критичності систем і внутрішніх процедур.

Як має виглядати завдання на усунення

Актив → Проблема → Ризик → Спосіб усунення → Відповідальний → Дедлайн → Статус

Типові дії

- виправлення / оновлення ОС або прикладного ПЗ
- зміна конфігурації або правил доступу
- закриття порту / відключення служби
- сегментація або компенсуючі заходи
- заміна застарілого продукту

7. ПОВТОРНА ПЕРЕВІРКА ПІСЛЯ ВИПРАВЛЕННЯ

Закрити задачу в Jira або Service Desk недостатньо. Потрібно технічно підтвердити, що проблема зникла.

Повторна перевірка має відповісти на три питання

01 **Чи зникла вразливість?**

02 **Чи правильно застосовано виправлення?**

03 **Чи не створило виправлення нових проблем?**

Правило закриття

Лише після успішної повторної перевірки вразливість доцільно переводити в статус «Усунено».

Історія підтвердження для критичних і високих ризиків

Дата виявлення	→	Власник	→	Усунення	→	Дата виправлення	→	Повторна перевірка	→	Результат

Такий ланцюжок дозволяє відрізнити «задача закрита» від «ризик справді усунено».

8. ПОСТІЙНИЙ МОНІТОРИНГ

Управління вразливостями не про щоквартальний Excel. Процес має працювати постійно та реагувати на зміни.

Тригери для повторного циклу

Нова критична CVE (Common Vulnerabilities and Exposures)

Перевірити, чи є уразливий компонент у вашій інфраструктурі.

Зміна інфраструктури

Нові сервери, сервіси, сегменти, домени або правила доступу.

Новий сервіс / реліз

Додати актив у реєстр та перевірити перед або після запуску.

Міграція у хмару

Повторно оцінити exposure та конфігурації.

Оновлення критичної системи

Переконатися, що оновлення не створило нових проблем.

Кіберінцидент

Перевірити пов’язані активи, вектори атаки та аналогічні слабкі місця.

Ключовий принцип

Система, яка вчора не мала відомих критичних проблем, сьогодні вже може бути в зоні ризику. Тому важливі не лише календарні перевірки, а й подієві тригери.

Що контролювати постійно

- нові активи та зміни зовнішньої доступності
- нові критичні вразливості
- прострочені завдання на усунення
- виконання SLA та винятки

9. ЗВІТНІСТЬ ДЛЯ КОМАНДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КЕРІВНИЦТВА

Одна таблиця з CVE (Common Vulnerabilities and Exposures) не відповідає на головне питання керівництва: «Чи зменшується наш кіберризик?»

Що показувати

- загальна кількість активів і покриття скануванням
- Критичний / Високий / Середній / Низький
- прострочені критичні та високі
- середній час усунення
- динаміка ризику та найбільш ризикові активи
- нові й усунені вразливості за період
- винятки та прийняті ризики

Приклад управлінського повідомлення

За місяць усунено 83% критичних вразливостей. 4 критичні проблеми залишаються відкритими. 2 з них стосуються зовнішньо доступних систем та перевищили внутрішній SLA.

Два рівні звітності

Для ІБ / ІТ

Технічні деталі, активи, CVE, статуси усунення, строки, повторна перевірка, винятки.

Для керівництва

Ризик, динаміка, проблемні активи, прострочення, тренд і рішення, які потребують управлінської уваги.

Що варто мати як доказ роботи процесу

Зріле управління вразливостями — це не лише технічний сканер. Важливо мати можливість показати історію від виявлення проблеми до її підтвердженого закриття.

- **Актуальний реєстр активів**
- **Власники критичних систем**
- **Внутрішня процедура управління вразливостями**
- **Правила оцінювання ризику**
- **Матриця пріоритезації**
- **Встановлені SLA**
- **Історія сканувань**
- **Завдання на усунення**
- **Підтвердження повторна перевірка**
- **Прийняття ризику та винятки**
- **Регулярна звітність**
- **Історія зміни статусів**

Практична перевірка

Якщо під час внутрішньої оцінки інформацію доводиться вручну збирати з Excel, Jira, електронної пошти та кількох систем то процес є, але він погано керований і складний для доказів.

Чекліст для самоперевірки

Спробуйте відповісти «так» на кожне питання. Якщо на кілька пунктів відповідь «ні» то процес потребує вдосконалення.

- ☐ Маємо актуальний реєстр IT-активів.
- ☐ Знаємо всі активи, доступні з Інтернету.
- ☐ Для критичних активів визначені власники.
- ☐ Вразливості шукаються регулярно.
- ☐ Отримуємо інформацію про нові критичні CVE.
- ☐ Оцінюємо не лише CVSS, а й бізнес-ризик.
- ☐ Встановлені строки для критичних, високих, середніх і низьких ризиків.
- ☐ Для критичних вразливостей є відповідальний.
- ☐ Бачимо прострочені завдання на усунення.
- ☐ Після виправлення виконується повторна перевірка.
- ☐ Можемо показати підтвердження повторна перевірка.
- ☐ Керівництво регулярно отримує звітність.
- ☐ Фіксуємо винятки та прийняті ризики.
- ☐ Можемо показати повну історію від виявлення до перевірки.

Де в цьому процесі допомагає Holm Security?

Платформа допомагає централізувати технічну частину управління вразливостями: від виявлення активів до повторної перевірки та звітності.

Етап	Завдання	Як допомагає Holm Security
Виявлення	Знати активи	Виявлення та облік активів
Сканування	Знаходити слабкі місця	Регулярне сканування
Оцінка	Оцінювати ризик	Аналіз знайдених вразливостей
Пріоритезація	Визначати пріоритет	Ризик-орієнтована пріоритезація
Усунення	Контролювати усунення	Централізований контроль процесу
Перевірка	Перевіряти результат	Повторні перевірки
Звітність	Показувати стан ризику	Звіти та централізоване представлення

Що рішення не замінює

Holm Security не замінює управлінські рішення, внутрішні політики, юридичну оцінку відповідності або сам факт належної організації процесу. Рішення допомагає підтримати технічні та процесні етапи управління вразливостями.

Що отримує команда

- єдине уявлення про активи та поверхню атаки
- видимість критичних проблем і пріоритетів
- контроль усунення та повторних перевірок
- історію й звітність для внутрішнього контролю

Головне

Відповідність починається не зі звіту. Вона починається з процесу.

Компанія має в будь-який момент розуміти: що ми захищаємо → які ризики маємо → що є критичним → хто це виправляє → коли → чи було проблему справді усунено.

Наступний крок

Перевірте, чи можете ви швидко показати:

- актуальний реєстр активів
- відкриті критичні та високі вразливості
- відповідальних і строки усунення
- прострочені завдання та винятки
- результати повторної перевірки

Якщо відповідь «ні»

Процес можна суттєво спростити та автоматизувати. **Holm Security** допомагає централізувати виявлення, оцінювання, пріоритезацію та контроль усунення вразливостей.

КОНТАКТИ SOFTICO

Потрібна допомога з управлінням кіберризиками?

Фахівці SOFTICO допоможуть оцінити поточний стан захисту, визначити пріоритетні ризики та підібрати рішення Holm Security під вашу інфраструктуру.

Сайт
softico.ua

Телефон
+38 (044) 383-44-10

Пошта
info@softico.ua

SOFTICO — Value Added IT-дистриб’ютор в Україні

Зв’яжіться з нами: Консультація • підбір рішення • підтримка

Підготовлено станом на 29 жовтня 2026 року. Перед використанням перевірте чинні консолідовані редакції актів і вимоги, що поширюються саме на вашу установу. Цей матеріал має інформаційний характер і не є офіційним роз’ясненням НБУ, юридичною консультацією, аудиторським висновком або підтвердженням відповідності.