Лабораторна робота №2

Аналіз та оцінювання ризиків інформаційної безпеки

Мета – визначити характеристики ризиків по відношенню до інформаційної системи та її ресурсів та обрати необхідні захисні засоби.

Фактори, що враховуються при оцінюванні ризиків

- Цінність ресурсів,
- Оцінка значимості загроз
- Оцінка значимості вразливостей
- Ефективність засобів захисту

Визначення

Базовий рівень безпеки (Baseline Security) – обов’язковий мінімальний рівень захищеності для інформаційної системи

Завдання для самостійної підготовки– ознайомитись та зробити огляд критеріїв для визначення базового рівня безпеки.

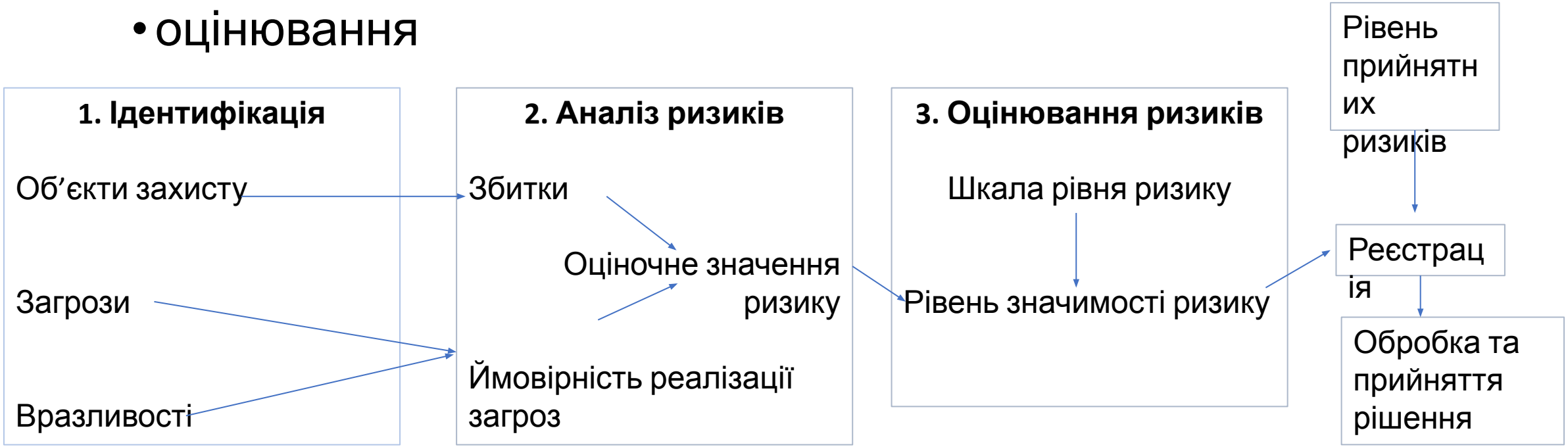
Базовий аналіз ризиків – аналіз ризиків, що проводиться у відповідності з вимогами базового рівня захищеності. Використовується у випадках, коли інформаційна до системи немає підвищених вимог щодо інформаційної безпеки.

Повний аналіз ризиків – аналіз ризиків для інформаційних систем до яких є підвищенні вимоги в галузі інформаційної безпеки. Обов’язково вміщує **визначення цінності** інформаційних ресурсів, оцінку загроз та вразливостей, вибір адекватних контрзаходів, **оцінку їх ефективності**.

- При аналізі ризиків збитки, що очикуються у вападку реалізації загроз порівнюються з витратами на заходи безпеки. Надалі приймається рішення щодо ризику що оцінюється, який може бути
- Знижений, за рахунок використання заходам захисту
- Усунений, за рахунок відмови від використання ресурсу, що схильний до загрози
- Перенесений (наприклад, за рахунок страхування)
- Прийнятний

Етапи оцінювання ризиків

- Ідентифікація
- Аналіз
- оцінювання



Завдання

1. **Провести перший етап процесу аналізу ризиків**

- Скласти перелік та опис елементів ризику: об’єктів захисту, загроз, вразливостей

Приклади об’єктів захисту: інформаційні активи, програмне забезпечення, фізичні активи, сервіси, людські ресурси, нематеріальні ресурси – репутація та імідж організації.

Дані для процесу ідентифікації можна отримати

- з результатів аудиту,
- даних про події та інциденти,
- як експертне оцінювання користувачами, спеціалістами з інформаційної безпеки, ІТ спеціалістів, зовнішніх консультантів тощо.