**Лекція 6**

# ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ IoT

**Зміст**



У цій лекції ми розглянемо ключові аспекти безпеки систем IoT, проблеми, з якими стикаються ці системи, а також способи забезпечення захисту від різних загроз.

---

## 2. Основні загрози безпеці в IoT

1. **Незахищені пристрої**:
   - Багато IoT-пристроїв мають обмежені можливості для встановлення ефективних механізмів безпеки. Вони можуть мати слабкі паролі, відсутність можливості оновлення програмного забезпечення або уразливості, які можуть бути використані зловмисниками.
2. **Невикористані або слабкі механізми аутентифікації**:
   - Деякі пристрої можуть не підтримувати належні механізми аутентифікації або використовувати прості паролі, що робить їх вразливими до атак за допомогою брутфорсу або інших методів злому.
3. **Інтерсепція та витік даних**:
   - Оскільки багато IoT-систем передають дані через бездротові мережі, ці дані можуть бути перехоплені зловмисниками, особливо якщо передача не зашифрована.
4. **Відсутність оновлень програмного забезпечення**:
   - Якщо пристрої не отримують регулярних оновлень безпеки, зловмисники можуть використати старі вразливості для атак.
5. **Атаки на мережу**:

- IoT-пристрої можуть стати частиною розподілених атак типу **DDoS (Distributed Denial of Service)**, коли вони використовуються для виведення з ладу серверів або мереж шляхом надмірного навантаження.

6. **Незахищені сервіси хмарних платформ**:
   - Враховуючи, що багато IoT-систем зберігають дані в хмарі, порушення безпеки цих сервісів може призвести до витоку даних або маніпуляцій з ними.

---

## 3. Основні принципи забезпечення безпеки IoT

1. **Шифрування**:
   - Шифрування є одним із ключових засобів захисту даних при передачі через мережі. Для забезпечення конфіденційності даних необхідно використовувати **TLS** (Transport Layer Security) або **SSL** (Secure Sockets Layer) для шифрування переданих даних між пристроями та хмарою або іншими пристроями.
2. **Аутентифікація та авторизація**:
   - Для кожного пристрою необхідно використовувати ефективні механізми аутентифікації, такі як **паролі, токени, сертифікати** або **біометричні дані**. Для забезпечення доступу до даних можна використовувати **механізми контролю доступу** на основі ролей (RBAC) або принцип найменших прав доступу (Least Privilege).
3. **Безпечне оновлення програмного забезпечення**:
   - Всі IoT-пристрої повинні отримувати регулярні оновлення безпеки, які закривають відомі вразливості. Важливо використовувати безпечні канали для оновлення програмного забезпечення, щоб уникнути атак через фальшиві оновлення.
4. **Ізоляція пристроїв і мереж**:
   - Для підвищення безпеки IoT можна використовувати мережеву ізоляцію, щоб кожен пристрій або група пристроїв не могла мати доступ до іншої частини мережі без належної аутентифікації. Це знижує ймовірність проникнення зловмисників через один пристрій до інших частин системи.
5. **Моніторинг і аналіз трафіку**:
   - Системи IoT повинні бути налаштовані на постійний моніторинг трафіку та виявлення підозрілих активностей, таких як незвичайна кількість запитів або спроби несанкціонованого доступу. Можна використовувати системи аналізу великих даних (Big Data) та інструменти на базі штучного інтелекту для виявлення аномалій.

---

## 4. Технічні рішення для забезпечення безпеки IoT

1. **Безпечна архітектура IoT**:
   - **Безпечний дизайн** системи IoT має бути одним із перших кроків при розробці. Це включає планування на етапі архітектури для використання шифрування, захисту доступу та ізоляції даних.
   - Створення **рівнів безпеки** дозволяє забезпечити захист на всіх етапах передачі даних — від пристрою до серверу.
2. **Додаткові засоби безпеки на пристроях**:
   - Використання **апаратних модулів безпеки** (HSM — Hardware Security Module) дозволяє зберігати ключі та сертифікати в захищеному середовищі, що знижує ймовірність їх викрадення.
   - Встановлення **довірених платформ** на пристрої, що дозволяє перевіряти їх цілісність і захищати від несанкціонованих змін.
3. **Мережеві протоколи безпеки для IoT**:
   - Використання сучасних протоколів для безпеки в мережі, таких як **IPsec**, **VPN** та **TLS/SSL** для захисту даних, що передаються по відкритих мережах.
   - Механізми аутентифікації, такі як **OAuth 2.0** або **OpenID**, можуть бути використані для забезпечення безпеки при авторизації користувачів.

---

## 5. Політики безпеки та управління ризиками

1. **Політики захисту даних**:
   - Встановлення чітких політик з безпеки даних є важливою складовою частиною забезпечення безпеки в IoT. Це включає визначення, які дані мають бути захищені, як вони повинні оброблятися та зберігатися, а також хто має доступ до цих даних.
2. **Ризик-менеджмент**:
   - Оцінка ризиків та визначення ймовірних загроз допомагає приймати необхідні заходи для захисту IoT-систем. Ризик-менеджмент включає в себе ідентифікацію потенційних уразливостей та розробку стратегій для їх усунення.
3. **Навчання користувачів і адміністраторів**:
   - Один з ключових аспектів безпеки — це **освічені користувачі та адміністратори**, які розуміють основні загрози та вміють захищати пристрої і дані.

---

## 6. Висновок

Безпека систем IoT є надзвичайно важливою через великий обсяг переданих і оброблюваних даних, а також через потенційні ризики для приватності та цілісності інформації. Захист від кібератак, шифрування даних, використання сучасних методів аутентифікації, регулярні оновлення програмного забезпечення та аналіз трафіку — все це необхідні елементи для забезпечення надійної безпеки систем IoT. Лише за умови комплексного підходу до забезпечення безпеки можна гарантувати належний захист IoT-пристроїв і даних користувачів.