Безпека операційних систем і комп'ютерних мереж

Лекція 6

ISO/IEC 15408
“Common Criteria”

Історія розроблення (1/3)

- **1990 рік**: Міжнародна організація із стандартизації (ISO) розпочинає роботи із створення стандарту у сфері оцінки безпеки інформаційних технологій (ІТ). Основні цілі розробки:
  - уніфікація національних стандартів у сфері оцінки безпеки ІТ
  - підвищення рівня довіри до оцінки безпеки ІТ
  - скорочення витрат на оцінку безпеки ІТ на основі взаємного визнання сертифікатів
- **Червень 1993 року**: організації із стандартизації та забезпеченню безпеки США, Канади, Великої Британії, Франції, Германії та Нідерландів об’єднали свої зусилля в рамках проекту із створення єдиної сукупності критеріїв оцінки безпеки ІТ. Цей проект отримав назву “Загальні критерії" (ЗК). Задача Загальних критеріїв – забезпечити взаємне визнання результатів стандартизованої оцінки безпеки на світовому ринку ІТ.

Історія розроблення (2/3)

- **Січень 1996 року**: Завершена розробка версії 1.0 “Загальних критеріїв” (ЗК)
- **Квітень 1996 року**: Версія 1.0 ЗК ухвалена ISO
- Було проведено ряд експериментальних оцінок на основі версії 1.0 ЗК, а також організовано широке обговорення документу
- **Травень 1998 року**: Оприлюднена версія 2.0 ЗК
- **Червень 1999 року**: На основі версії 2.0 ЗК прийнято міжнародний стандарт **ISO/IEC 15408**
- **1 грудня 1999 року**: Виданий офіційний текст стандарту.
- Зміни, що були внесені в стандарт на завершальній стадії його прийняття, враховані у версії 2.1 ЗК, що ідентична стандарту за змістом

Історія розроблення (3/3)

- Вже після прийняття стандарту з урахуванням досвіду його використання з'явився ряд інтерпретацій ЗК, які після розгляду Комітетом з інтерпретацій (CCIMB) приймаються, офіційно оприлюднюються та набувають чинності як діючі зміни й доповнення до ЗК
- **2005 рік**: Версія 2.2 ЗК стала основою для внесення змін у стандарт ISO. Версію стандарту позначили як **ISO/IEC 15408:2005**. Ідентична їй за змістом версія ЗК – 2.3
- Протягом певного часу паралельно проводили урахування інтерпретацій (була завершена версія 2.4 ЗК і розроблювали версію 2.6 ЗК) і вели розробку версії 3.0 ЗК, яка має дещо змінену (спрощену) структуру вимог
- 2008 рік: замість очікуваної версії 2.4 ЗК в якості стандарту **ISO/IEC 15408:2008** ухвалили версію 3.0 ЗК.
- Методологія застосування ЗК оформлена у вигляді окремого документа "Загальна методологія оцінювання безпеки інформаційних технологій" і також набула статусу стандарту, діюча версія: **ISO/IEC 18045:2005**

Основні відомості

- Стандарт ISO/IEC 15408 регламентує усі стадії розробки, кваліфікаційного аналізу та експлуатації продуктів інформаційних технологій
- Стандарт пропонує досить складну і бюрократичну концепцію процесу розробки і кваліфікаційного аналізу продуктів ІТ
- У застосуванні до оцінки безпеки продуктів інформаційних технологій (ПІТ) стандарт є по суті метазасобом, що задає систему понять, в термінах яких повинна проводитись оцінка
- Стандарт містить відносно повний каталог вимог безпеки (функціональних та гарантій), але не надає конкретних наборів вимог та критеріїв для тих чи інших типів ПІТ, виконання яких необхідно перевіряти
- Вимоги та критерії формулюються у *профілях захисту* (ПЗ) та *завданнях з безпеки* (ЗБ)
- Саме офіційно прийняті профілі захисту утворюють побудовану на основі ЗК нормативну базу, що використовується на практиці у сфері інформаційної безпеки

Структура Загальних критеріїв

- ЗК є сукупністю самостійних, але взаємопов'язаних частин

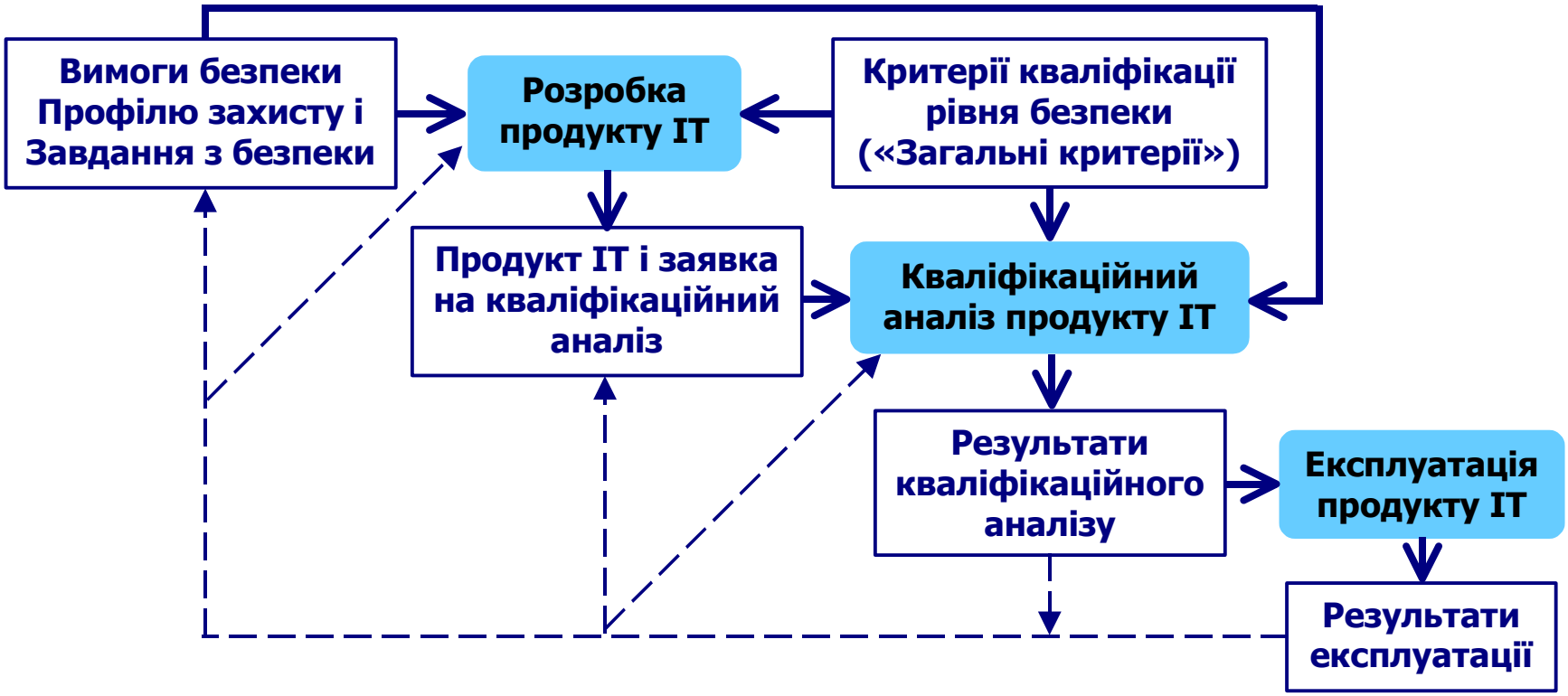
1) Розділ **Представлення і загальна модель** – визначає загальну концепцію й принципи оцінки безпеки ІТ і подає загальну модель оцінки, а також конструкції для:
   - формування задач захисту ІТ
   - вибору й визначення вимог безпеки ІТ
   - опису специфікацій високого рівня для продуктів і систем.
2) Розділ **Вимоги до функцій безпеки** – встановлює набір функціональних компонентів як стандартний шлях формулювання функціональних вимог до об'єктів оцінки
3) Розділ **Вимоги гарантій безпеки** – включає компоненти вимог гарантій оцінки, а також рівні гарантій оцінки, які визначають ранжирування за ступенем задоволення вимог

- Був передбачений розділ **Визначені профілі захисту,** що містив приклади профілів захисту, які включали функціональні вимоги безпеки та вимоги гарантій оцінки, що були ідентифіковані у вихідних критеріях (ITSEC, CTCPEC, FC, TCSEC), а також інші профілі. **Цей розділ був вилучений із ЗК** починаючи з версії 2.0 (тобто, до складу стандарту ISO не увійшов). Але самі профілі існують і використовуються.

Базові поняття

- Задачі захисту (Security Objectives)
  - Потреба споживачів продукту IT
    - у протистоянні заданій множині загроз безпеці
    - у необхідності реалізації політики безпеки
- Профіль захисту (Protection Profile)
  - Спеціальний нормативний документ, що містить:
    - задачі захисту,
    - функціональні вимоги,
    - вимоги адекватності,
    - їхнє обґрунтування.
  - Служить керівництвом для розроблювача при створенні завдання з безпеки
- Завдання з безпеки (Security Target)
  - Спеціальний нормативний документ, що містить:
    - задачі захисту,
    - функціональні вимоги,
    - вимоги адекватності,
    - загальні специфікації засобів захисту,
    - їхнє обґрунтування.
  - У ході кваліфікаційного аналізу служить як опис продукту IT

Процес розробки та кваліфікаційного аналізу



Матеріали для проведення кваліфікаційного аналізу

- Завдання з безпеки, що описує функції захисту продукту ІТ і вимоги безпеки, що відповідають вимогам Профілю захисту, на реалізацію якого претендує продукт ІТ
- Докази можливостей продукту ІТ, представлені його розроблювачем
- Продукт ІТ
- Додаткові відомості, отримані шляхом проведення різних експертиз

Три стадії процесу кваліфікаційного аналізу

1. Аналіз Профілю захисту на предмет
   - його повноти,
   - несуперечності,
   - можливості реалізації та
   - можливості використання як набору вимог для продукту, що аналізують
2. Аналіз Завдання з безпеки на предмет
   - його відповідності вимогам профілю захисту,
   - повноти,
   - несуперечності,
   - можливості реалізації та
   - можливості використання як опису продукту ІТ
3. Аналіз продукту ІТ на предмет відповідності Завданню з безпеки

Структура профілю захисту (1/7)

- Вступ
  - Ідентифікатор
  - Огляд змісту
- Опис ПІТ
- Середовище експлуатації
  - Загрози безпеці
  - Політика безпеки
  - Умови експлуатації
- Задачі захисту
  - Задачі захисту ПІТ
  - Інші задачі захисту
- Функціональні вимоги
- Вимоги гарантій
- Вимоги до середовища експлуатації
- Додаткові відомості
- Обґрунтування
  - Обґрунтування задач захисту
  - Обґрунтування вимог безпеки

Структура профілю захисту (2/7)

- Вступ

  Інформація, необхідна для пошуку профілю в бібліотеці профілів

  - Ідентифікатор

    Унікальне ім'я, придатне для пошуку серед подібних профілів і для посилань на нього

  - Огляд змісту

    Коротка анотація профілю захисту, на підставі якої споживач може зробити висновок про придатність даного профілю для його потреб

- Опис ПІТ

  Коротка характеристика, функціональне призначення, принципи роботи, методи використання і т.д. Ця інформація не підлягає аналізу і сертифікації

Структура профілю захисту (3/7)

- Середовище експлуатації

  Опис усіх аспектів функціонування ПІТ, пов'язаних з безпекою

  - Загрози безпеці

    Опис загроз безпеці, яким повинний протистояти захист. Для кожної загрози: джерело, метод впливу, об'єкт.

  - Політика безпеки

    Визначення і пояснення (при необхідності) правил політики безпеки

  - Умови експлуатації

    Вичерпна характеристика середовища експлуатації з погляду безпеки

Структура профілю захисту (4/7)

- Задачі захисту

  Потреби користувачів у протидії зазначеним загрозам безпеці та/або в реалізації політики безпеки

  - Задачі захисту ПІТ
  - Інші задачі захисту

Структура профілю захисту (5/7)

- Вимоги безпеки

  Вимоги безпеки, яким повинний задовольняти ПІТ для рішення задач захисту

  - Функціональні вимоги

    Тільки типові вимоги, передбачені відповідними розділами «Загальних критеріїв». Можуть наказувати чи забороняти використання конкретних методів і засобів

  - Вимоги гарантій

    Також тільки типові вимоги

  - Вимоги до середовища експлуатації

    Необов'язковий розділ. Функціональні вимоги та/або вимоги гарантій до середовища експлуатації. Використання типових вимог є бажаним, але не обов'язковим

Структура профілю захисту (6/7)

- Додаткові відомості

  Необов'язковий розділ

- Обґрунтування

  Демонстрація того, що профіль захисту містить повну і зв'язну множину вимог, і що ПІТ, який їм задовольняє, буде ефективно протистояти загрозам безпеці середовища експлуатації

  - Обґрунтування задач захисту

    Демонстрація того, що задачі захисту, запропоновані в профілі, відповідають властивостям середовища експлуатації

  - Обґрунтування вимог безпеки

    Демонстрація того, що вимоги безпеки дозволяють вирішити задачі захисту

Структура профілю захисту (7/7)

Для обґрунтування вимог безпеки демонструють, що:

- Сукупність цілей, переслідуваних окремими функціональними вимогами, відповідає встановленим задачам захисту
- Вимоги безпеки є погодженими (не суперечать одна одній)
- Усі взаємозв'язки між вимогами враховані або за допомогою їхньої вказівки у вимогах, або за допомогою встановлення вимог до середовища експлуатації
- Обраний набір вимог і рівень гарантій можуть бути обґрунтовані

Структура Завдання з безпеки (1/10)

- Вступ
  - Ідентифікатор
  - Огляд змісту
  - Заявка на відповідність ЗК
- Опис ПІТ
  - Середовище експлуатації
  - Загрози безпеці
  - Політика безпеки
  - Умови експлуатації
- Задачі захисту
  - Задачі захисту ПІТ
  - Інші задачі захисту
- Вимоги безпеки
  - Функціональні вимоги
  - Вимоги гарантій
  - Вимоги до середовища експлуатації
- Загальні специфікації продукту ІТ
  - Специфікації функцій захисту
  - Специфікації рівня гарантій
  - Заявка на відповідність профілю захисту
  - Посилання на профіль захисту
  - Відповідність профілю захисту
  - Удосконалення профілю захисту
- Обґрунтування
  - Обґрунтування задач захисту
  - Обґрунтування вимог безпеки
  - Обґрунтування функцій захисту
  - Обґрунтування рівня гарантій
  - Обґрунтування відповідності профілю захисту

Структура Завдання з безпеки (2/10)

- Вступ

  Інформація, необхідна для ідентифікації Завдання з безпеки, визначення призначення, а також огляд його змісту

  - Ідентифікатор

    Унікальне ім'я, необхідне для пошуку й ідентифікації Завдання з безпеки і відповідного йому ПІТ

  - Огляд змісту

    Докладна анотація Завдання з безпеки, на підставі якої споживач може зробити висновок про придатність ПІТ для рішення його задач

  - Заявка на відповідність ЗК

    Опис усіх властивостей ПІТ, що підлягають кваліфікаційному аналізу на основі ЗК

Структура Завдання з безпеки (3/10)

- Опис ПІТ
  - Середовище експлуатації
  - Загрози безпеці
  - Політика безпеки
  - Умови експлуатації
- Задачі захисту
  - Задачі захисту ПІТ
  - Інші задачі захисту

    Вищезазначені розділи збігаються з однойменними розділами профілю захисту

Структура Завдання з безпеки (4/10)

- Вимоги безпеки

  Вимоги безпеки, якими керувався розроблювач ПІТ, що дозволяє йому заявляти про успішне рішення задач захисту

  - Функціональні вимоги

    На відміну від відповідного розділу профілю захисту, допускається використання крім типових вимог ЗК інших, специфічних для даного продукту і середовища його експлуатації

  - Вимоги гарантій

    Може включати рівні гарантій, не передбачені в ЗК

  - Вимоги до середовища експлуатації

    Необов'язковий розділ

Структура Завдання з безпеки (5/10)

- Загальні специфікації ПІТ

  Відображення реалізації ПІТ вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту

  - Специфікації функцій захисту

    Опис функціональних можливостей засобів захисту ПІТ, що заявлені розроблювачем як ті, що реалізують вимоги безпеки. Форма представлення специфікацій повинна дозволяти визначати відповідності між функціями захисту і вимогами безпеки

  - Специфікації рівня гарантій

    Визначення заявленого рівня гарантій захисту ПІТ і його відповідність вимогам гарантій у вигляді подання параметрів технології проектування і створення ПІТ

Структура Завдання з безпеки (6/10)

- Заявка на відповідність профілю захисту

  Необов'язковий пункт. Завдання з безпеки претендує на задоволення вимог одного чи декількох профілів захисту, для кожного з яких цей розділ повинний містити таку інформацію:

  - Посилання на профіль захисту

    Однозначно ідентифікує профіль захисту, на реалізацію якого претендує Завдання з безпеки. Реалізація профілю захисту передбачає коректну реалізацію всіх його вимог без винятку.

  - Відповідність профілю захисту

    Можливості ПІТ, що реалізують задачі захисту і вимоги, що містяться в профілі захисту

  - Удосконалення профілю захисту

    Можливості ПІТ, що виходять за рамки профілю

Структура Завдання з безпеки (7/10)

- Обґрунтування

  Демонстрація того, що Завдання з безпеки містить повну і зв'язну множину вимог, що ПІТ, який його реалізує, буде ефективно протистояти загрозам безпеці середовища експлуатації, і що загальні специфікації функцій захисту відповідають вимогам безпеки

  - Обґрунтування задач захисту

    Демонстрація того, що задачі захисту, запропоновані в Завданні з безпеки, відповідають властивостям середовища експлуатації

Структура Завдання з безпеки (8/10)

- Обґрунтування вимог безпеки

  Демонстрація того, що вимоги безпеки дозволяють вирішити задачі захисту. Необхідно показати, що:

  - Функціональні вимоги безпеки відповідають задачам захисту
  - Вимоги гарантій відповідають функціональним вимогам і підсилюють їх
  - Сукупність усіх функціональних вимог забезпечує рішення задач захисту
  - Усі взаємозв'язки між вимогами ЗК враховані або за допомогою зазначення їх у вимогах, або за допомогою встановлення вимог до середовища експлуатації
  - Усі вимоги безпеки успішно реалізовані
  - Заявлений рівень гарантій може бути підтверджений

Структура Завдання з безпеки (9/10)

- Обґрунтування функцій захисту

  Демонстрація того, що функції захисту відповідають функціональним вимогам безпеки і задачам захисту. Повинно бути показано, що:

  - Зазначені функції захисту відповідають заявленим задачам захисту
  - Сукупність зазначених функцій захисту забезпечує ефективне рішення сукупності задач захисту
  - Заявлені можливості функцій захисту відповідають дійсності

- Обґрунтування рівня гарантій

  Підтвердження, що заявлений рівень безпеки відповідає вимогам гарантій

Структура Завдання з безпеки (10/10)

- Обґрунтування відповідності профілю захисту

  Демонстрація того, що вимоги Завдання з безпеки підтримують усі вимоги профілю захисту. Повинно бути показано, що:

  - Всі удосконалення задач захисту у порівнянні з профілем захисту здійснені коректно й у напрямку їхнього розвитку і конкретизації
  - Всі удосконалення вимог безпеки в порівнянні з профілем захисту здійснені коректно й у напрямку їхнього розвитку і конкретизації
  - Усі задачі захисту профілю захисту успішно вирішені і усі вимоги профілю захисту задоволені
  - Ніякі додатково введені Завдання з безпеки спеціальні задачі захисту і вимоги безпеки не суперечать профілю захисту

Структура вимог

- Функціональні вимоги та вимоги гарантій подані в одному спільному стилі та використовують одну і ту саму організацію та термінологію
- Термін **клас** використовується для найбільш загального групування вимог безпеки. Усі члени класу поділяють спільний намір при різниці в охопленні цілей безпеки.
- Члени класу названі **сімействами**. Сімейство – це групування наборів вимог безпеки, які забезпечують виконання певної частини цілей безпеки, але можуть відрізнятись в акценті або жорсткості.
- Члени сімейства названі **компонентами**. Компонент описує визначений набір вимог безпеки – найменший набір вимог безпеки, що обирається для включення у структури, визначені в ЗК.
- Компоненти побудовані з **елементів**. Елемент – найнижчий і неподільний рівень вимог безпеки, на якому проводиться оцінка їх виконання.

Перетворення компонентів

- Компоненти можуть бути перетворені за допомогою дозволених дій, щоби забезпечити виконання певної політики безпеки або протистояти певній загрозі. Не усі дії припустимі на усіх компонентах. Кожний компонент ідентифікує і визначає дозволені дії або обставини, за яких дія може застосовуватись до компонента, а також результати застосування дії.
- До дозволених дій належать: призначення, вибір і обробка
- **Призначення** дозволяє заповнити специфікацію ідентифікованого параметра при використанні компонента. Параметр може бути ознакою або правилом, що конкретизує вимоги до певної величини або діапазону величин.
- **Вибір** – це дія вибору одного чи більшої кількості пунктів із списку, щоби конкретизувати можливості елементу
- **Обробка** дозволяє включити додаткові деталі в елемент, і передбачає інтерпретацію вимоги, правила, константи або умови, засновану на задачах захисту. Обробка повинна лише обмежувати набір можливих функцій або механізмів, щоби здійснити вимоги, але не збільшувати їх. Обробка не дозволяє створювати нові вимоги або видаляти існуючі, і не впливає на список залежностей, що пов’язані з компонентом.

Набори структур

- ЗК визначають набори структур, що поєднують компоненти вимог безпеки
- Проміжна комбінація компонентів названа **пакетом**. Пакет включає набір вимог, які забезпечують виконання піднабору задач захисту.
- Пакет призначений для багаторазового використання
- Пакет визначає вимоги, які є необхідними для досягнення ідентифікованих задач
- Пакет може використовуватись для формування Профілів захисту і Завдань з безпеки
- **Рівні гарантій оцінки** – це визначені пакети вимог гарантій. Рівень гарантій – це набір базових вимог гарантій для оцінки. **(EAL)**

Таксономія вимог
Функціональні вимоги – класи

- FAU – Аудит безпеки
  - Вимоги до розпізнання, реєстрації, зберігання та аналізу інформації, що пов’язана з діями, що стосуються безпеки об’єкта оцінювання (ОО)
- FCO – Інформаційний обмін
  - Вимоги до визначення ідентичності сторін, що беруть участь в обміні даними
- FCS – Криптографічна підтримка
- FDP – Захист інформації користувача
  - Вимоги до функцій безпеки ОО та політики функцій безпеки ОО, що пов’язані із захистом даних користувача
- FIA – Ідентифікація й автентифікація
  - Вимоги до функцій, що призначені для встановлення й перевірки ідентичності користувача
- FMT – Керування безпекою
  - Вимоги, що пов’язані з керуванням безпекою ОО
- FPR – Конфіденційність доступу до системи
  - Вимоги таємності, що забезпечують захист користувача від розкриття й невірного використання його ідентифікаторів іншими користувачами

Таксономія вимог
Функціональні вимоги – класи

- FPT – Захист функцій безпеки
  - Вимоги, що стосуються цілісності та контролю механізмів, що забезпечують функції безпеки, та цілісності й контролю даних функцій безпеки
- FRU – Контроль за використанням ресурсів
- FTA – Контроль доступу до системи
  - Функціональні вимоги, понад вимог ідентифікації й автентифікації, для керування сеансом роботи користувача
- FTP – Забезпечення прямої взаємодії
  - Вимоги до забезпечення надійного маршруту зв'язку між користувачами і функціями безпеки та надійного каналу зв'язку між функціями безпеки, що мають такі спільні характеристики:
    - маршрут комунікацій побудований із застосуванням внутрішніх і зовнішніх каналів комунікацій, що ізолюють ідентифікований піднабір даних та команд функцій безпеки від інших частин функцій безпеки та даних користувача;
    - використання маршруту комунікацій може бути ініційовано користувачем та/або функцією безпеки;
    - маршрут комунікацій здатний забезпечити гарантії того, що користувач взаємодіє з потрібною функцією безпеки і що функція безпеки взаємодіє з потрібним користувачем, тобто забезпечується надійна ідентифікація кінцевих пунктів.

Таксономія вимог
Вимоги гарантій – класи

- APE – Оцінка профілю захисту
  - Вимоги до оцінки профілю захисту з метою підтвердження того, що він є повним, несуперечливим, технічно вірним, і таким чином придатним для розробки завдань з безпеки і для занесення в реєстр
- ASE – Оцінка завдання з безпеки
  - Вимоги до оцінки завдання з безпеки з метою підтвердження того, що воно є повним, несуперечливим, технічно вірним, і таким чином придатним для використання в якості основи для оцінки відповідного ОО
- ADV – Розробка
  - Вимоги до процесу розробки, що дозволяють перевірити, чи були фактично відпрацьовані функції безпеки
- AGD – Документація
  - Вимоги до зрозумілості, повноти й завершеності експлуатаційної документації
- ALC – Підтримка життєвого циклу
  - Вимоги до прийняття добре визначеної моделі етапів життєвого циклу ОО
- ATE – Тестування
  - Вимоги до об’єму, глибини та виду тестування ОО
- AVA – Оцінка вразливості
  - Вимоги, що спрямовані на виявлення вразливих місць
- ACO – Інтеграція
  - Вимоги, що надають впевненості у тому, що інтегрований ОО буде функціонувати безпечно, якщо він спирається на функції захисту раніше оцінених компонентів