Безпека операційних систем і комп'ютерних мереж

Лекція 4

Стандарти оцінювання захищеності систем

Призначення стандартів інформаційної безпеки

- Викорінення вад захисту – це тактичний шлях побудови захищених систем, чи підхід “знизу”.
  - Дозволяє позбутися окремих уразливостей і підвищити захищеність системи
  - Не дозволяє оцінити ані повноту виконання цієї задачі, ані досягнутий рівень захисту
- Стандарти визначають стратегічний підхід до побудови захищених систем, або підхід “зверху”
  - Безпека системи – характеристика якісна, для неї не існує одиниць виміру
    - Різні фахівці запропонують різні шляхи підвищення захищеності системи і по-різному оцінять її
  - Єдиним способом встановити шкалу оцінки захищеності систем, а також узгодити погляди різних фахівців, є розробка стандарту
- Стандарт повинен регламентувати
  - концепції інформаційної безпеки,
  - підходи до її досягнення,
  - вимоги до систем і шляхи їх реалізації,
  - систему критеріїв оцінювання захищеності систем,
  - процедури оцінювання систем за цими критеріями.
- Стандарти створюють основу для погодження вимог
  - розробників систем,
  - споживачів (користувачів систем і власників інформації, що в них обробляється),
  - експертів, які оцінюють захищеність інформації в системах (а в разі необхідності – також і державних або відомчих органів, які видають дозвіл на експлуатацію системи і обробку в ній певної інформації).

Розвиток стандартів інформаційної безпеки

- TCSEC – Критерії оцінювання захищених комп'ютерних систем Міністерства оборони США («Оранжева книга»), 1983 р.
- ITSEC – Європейські критерії безпеки інформаційних технологій, 1991 р.
- "Руководящие документы Гостехкомиссии России", 1992 р.
- FCITS – Федеральні критерії безпеки інформаційних технологій США, 1992 р.

TCSEC (“Оранжева книга”)

- Trusted Computer System Evaluation Criteria. – US Department of Defense. – CSC-STD-001-83, 1983.
- Trusted Network Interpretation. – National Computer Security Center. NCSC-TG-005 Version 1, 1987.
- Trusted Database Management System Interpretation. – National Computer Security Center. NCSC-TG-021 Version 1, 1991.
- The Interpreted Trusted Computer System Evaluation Criteria Requirements. – National Computer Security Center. NCSC-TG-007-95, 1995.

TCSEC

- Визначення безпечної системи
  - система, що підтримує керування доступом таке, що лише уповноважені користувачі або процеси, що діють від їх імені, одержують можливість читати, записувати, створювати і знищувати інформацію
- 6 вимог до безпечної системи
  - Політика безпеки
  - Мітки безпеки
  - Ідентифікація і автентифікація
  - Реєстрація і облік
  - Коректність засобів захисту
  - Неперервність захисту

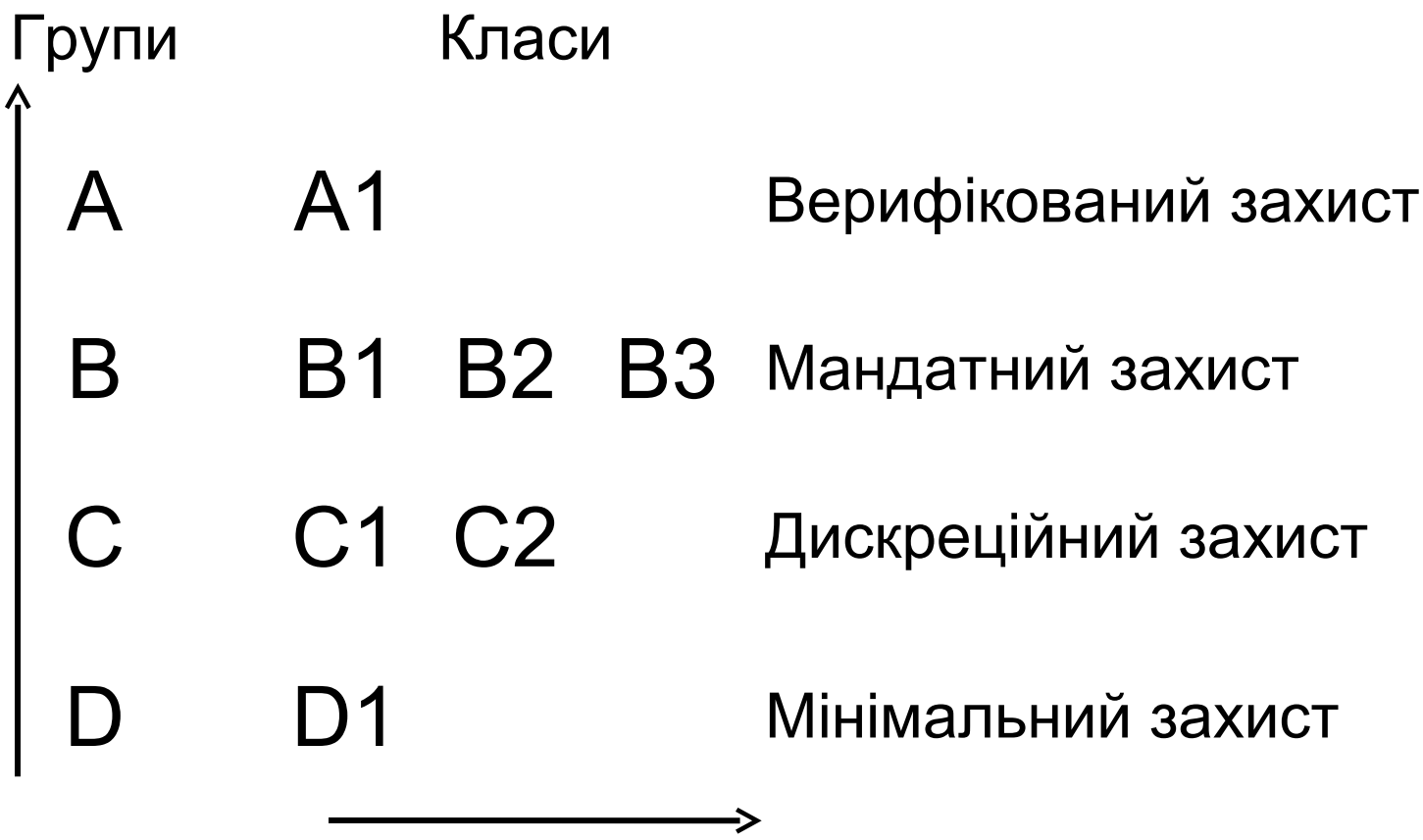
TCSEC: перелік вимог (1/2)

- Політика безпеки
  - Дискреційне керування доступом
  - Повторне використання об’єктів
  - **Мітки безпеки**
    - Цілісність міток безпеки
    - Експорт поміченої інформації
    - Мітки повноважень суб'єктів
    - Мітки пристроїв
  - Мандатне керування доступом
- Аудит
  - Ідентифікація і автентифікація
    - Прямае взаємодія з КЗЗ
  - Реєстрація і облік подій

TCSEC: перелік вимог (2/2)

- Коректність
  - **Коректність функціонування**
    - Архітектура системи
    - Цілісність системи
    - Аналіз прихованих каналів
    - Керування безпекою
    - Відновлення
  - **Коректність розробки**
    - Тестування безпеки
    - Розробка і верифікація специфікацій
    - Керування конфігурацією
    - Дистрибуція
- Документація
  - Настанова з безпеки користувача
  - Настанова адміністратора безпеки
  - Документування процесу тестування
  - Документування процесу розроблення

TCSEC: класифікація систем



Основні вимоги рівня С2 щодо операційних систем

- Засіб безпечного входу в систему, що вимагає унікальної ідентифікації користувачів і одержання ними повноважень доступу до комп'ютера тільки після того, як вони тим чи іншим способом пройдуть автентифікацію
- Дискреційне керування доступом, що дозволяє власнику ресурсу (наприклад, файлу) визначити, хто може отримати доступ до ресурсу і що він при цьому може з ним робити. Власник надає права, що дозволяють різні види доступу, окремому користувачу або групі користувачів.

Основні вимоги рівня С2 щодо операційних систем (2)

- Контроль (аудит) безпеки, що дозволяє виявляти і записувати події, які стосуються питань безпеки, або будь-які спроби створення системних ресурсів, а також звернення до них чи їх видалення. Записування ідентифікаторів під час входу в систему, що дозволяє встановлювати ідентичність усіх користувачів, спрощуючи тим самим відстежування будь-якого користувача, що намагається здійснити неавторизовану дію.
- Захист від повторного використання об'єкта, який не дозволяє користувачам переглядати дані, що були видалені іншим користувачем, або не дозволяє звертатись до пам'яті, яка раніше була використана, а далі звільнена іншим користувачем (“збирання сміття”). Захист від повторного використання об'єкта реалізується шляхом ініціалізації усіх об'єктів, включаючи файли і пам'ять, перед їх виділенням користувачеві.

Деякі важливі вимоги рівня B щодо операційних систем

- Механізм “довіреного маршруту”, який не дає троянським програмам можливості перехоплення імен і паролів користувачів при спробі їх входу в систему
  - Наприклад, у Windows механізм довіреного маршруту реалізований у формі “послідовності переносу уваги” на вход до системи Ctrl+Alt+Delete - secure attention sequence (SAS), яка не може бути перехопленою непривілейованими програмами. Ця клавіатурна послідовність завжди виводить екран безпеки Windows, яким керує система. SAS може також бути відправлена програмно шляхом використання API-функції SendSAS. При введенні SAS троянська програма, яка надає несправжнє діалогове вікно, будет обійдена.
- Довірений засіб керування, який вимагає підтримки ролей окремих облікових записів для здійснення адміністративних функцій. Наприклад, для адміністрування, для користувачів, що відповідають за резервне копіювання комп'ютера, і для звичайних користувачів надаються окремі облікові записи.

Висновки по TCSEC

- Перша спроба створити єдиний стандарт безпеки, що розрахований на розробників, споживачів і спеціалістів із сертифікації КС
- Орієнтований на системи спеціального (військового) застосування, головним чином на операційні системи (домінують вимоги з конфіденційності)
- Критерії гарантій реалізації засобів захисту і адекватності політики безпеки розроблені недостатньо
- Оцінка системи зводиться до перевірки виконання вимог одного з наперед визначених класів. Шкала класів є ієрархічною

ITSEC – Європейські критерії

- Information Technology Security Evaluation Criteria. Harmonized Criteria Of France-Germany-Netherlands-United Kingdom. – Department of Trade and Industry. – London, 1991.

- Відмова від єдиної універсальної шкали ступеня захищеності
- Вперше введено поняття гарантій (assurance) засобів захисту
  - Ефективність – відповідність між задачами захисту і реалізованим набором функцій (повнота і узгодженість)
  - Коректність – правильність і надійність реалізації функцій
- Додаткові вимоги з безпеки обміну даними

ITSEC – класи безпеки

- **F-C1**, **F-C2**, **F-B1**, **F-B2**, **F-B3** – відповідають TCSEC
- **F-IN** – підвищені вимоги до забезпечення цілісності (СКБД)
- **F-AV** – підвищені вимоги до забезпечення працездатності (системи реального часу)
- **F-DI** – розподілені системи з підвищеними вимогами до цілісності
- **F-DC** – розподілені системи з підвищеними вимогами до конфіденційності
- **F-DX** – розподілені системи з підвищеними вимогами до конфіденційності, цілісності і неможливості відмови від авторства

ITSEC – критерії гарантій

- Критерії ефективності
  - Відповідність набору засобів захисту заданим цілям
  - Взаємна узгодженість різних засобів і механізмів захисту
  - Здатність засобів захисту протистояти атакам
  - Можливість практичного використання недоліків архітектури засобів захисту
  - Простота використання засобів захисту
  - Можливість практичного використання функціональних недоліків засобів захисту

ITSEC – критерії гарантій

- Критерії коректності
  - Процес розроблення
    - Специфікація вимог безпеки
    - Розроблення архітектури
    - Створення робочого проекту
    - Реалізація
  - Середовище розроблення
    - Засоби керування конфігурацією
    - Використовувані мови програмування і компілятори
    - Безпека середовища розроблення
  - Експлуатаційна документація
    - Настанова користувача
    - Настанова адміністратора
  - Середовище експлуатації
    - Доставка і встановлення
    - Запуск и експлуатація

Висновки по ITSEC

- Головне досягнення – введення поняття гарантій захисту і визначення окремої шкали для критеріїв гарантій
- Відмова від єдиної ієрархічної шкали оцінювання систем
- ITSEC тісно пов'язані з TCSEC (не повністю самостійний документ)
- Визнання можливості наявності недоліків у сертифікованих системах і введення критерію можливості використання недоліків захисту

Руководящие документы ГТК России

- Концепция защиты средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации
- СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации
- Автоматизированные системы (АС). Защита от НСД к информации. Классификация АС и требования по защите информации

Руководящие документы ГТК России: классы СВТ и АС

- СВТ: 7 классов от 7 к 1
- АС: 3 группы, 9 классов
  - Группа 3
    АС, в которых работает один пользователь, допущенный ко всей информации. Классы 3Б и 3А
  - Группа 2
    АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации. Классы 2Б и 2А
  - Группа 1
    Многопользовательские АС, обрабатывается информация разных уровней конфиденциальности, пользователи имеют различные права доступа.
    Классы 1Д, 1Г, 1В, 1Б, 1А

Руководящие документы ГТК России: выводы

- Подобно «Оранжевой книге», документы ориентированы на системы военного применения
- Понятие «Политика безопасности» трактуется исключительно как поддержание режима секретности и отсутствие НСД. Средства защиты ориентируются исключительно на противодействие внешним угрозам
- Отсутствуют требования к защите от угроз работоспособности и к адекватности реализации политики безопасности. К структуре самой системы и к ее функционированию требования не предъявляются
- Используется единая универсальная шкала степени защищенности. Ранжирование требований по классам максимально упрощено

FCITS – «Федеральні критерії»: мета розробки

- Federal Criteria for Information Technology Security. – National Institute of Standards and Technology & National Security Agency. Version 1.0, 1992.

- Визначення універсального й відкритого для подальшого розвитку набору основних вимог безпеки, що висувають до сучасних інформаційних технологій
- Удосконалення існуючих вимог і критеріїв безпеки
- Узгодження між собою вимог і критеріїв безпеки інформаційних технологій, що прийняті у різних країнах
- Нормативне закріплення головних принципів інформаційної безпеки

FCITS – етапи розроблення продукту ІТ

1. Розроблення і аналіз профілю захисту
   - Вимоги, що викладені у профілі захисту, визначають функціональні можливості продуктів ІТ із забезпечення безпеки і умови експлуатації, за дотримання яких гарантується відповідність висунутим вимогам
   - Профіль захисту аналізують на повноту, несуперечність і технічну коректність
2. Розроблення і кваліфікаційний аналіз продуктів ІТ
   - Розроблені продукти ІТ піддають незалежному аналізу, мета якого – визначення ступеня відповідності характеристик продукту вимогам профілю захисту
3. Компонування і сертифікація системи оброблення інформації в цілому
   - Отримана в результаті система повинна задовольняти вимогам, що заявлені у профілі захисту

FCITS – структура профілю захисту

- Опис
  - Класифікаційна інформація, що необхідна для ідентифікації профілю у спеціальній картотеці
- Обґрунтування
  - Опис середовища експлуатації, загроз безпеці, що передбачаються, і методів використання продукту ІТ
- Функціональні вимоги до продукту ІТ
- Вимоги до технології розроблення продукту ІТ
- Вимоги до процесу кваліфікаційного аналізу продукту ІТ

FCITS – функціональні вимоги

- Реалізація політики безпеки
  - Політика аудита
    - Ідентифікація і автентифікація
    - Реєстрація в системі
    - Забезпечення прямої взаємодії з КЗЗ
    - Реєстрація і облік подій
  - Політика керування доступом
    - Дискреційне керування доступом
    - Мандатне керування доступом
    - Контроль прихованих каналів
  - Політика забезпечення працездатності
    - Контроль за розподілом ресурсів
    - Забезпечення стійкості до відмов
  - Керування безпекою
- Моніторинг взаємодій
- Логічний захист КЗЗ
- Фізичний захист КЗЗ
- Самоконтроль КСЗ
- Ініціалізація і відновлення КЗЗ
- Обмеження привілеїв під час роботи з КЗЗ
- Простота використання КЗЗ

FCITS – Вимоги до технології розробки

- Процес розроблення
  - Визначення множини функцій КЗЗ у відповідності до функціональних вимог
  - Реалізація КЗЗ
    - Визначення складу функціональних компонент КЗЗ
    - Визначення інтерфейсу КЗЗ
    - Декомпозиція КЗЗ на функціональні модулі
    - Структуризація КЗЗ на домени безпеки
    - Мінімізація функцій і структури КЗЗ
  - Гарантії реалізації КЗЗ
  - Тестування і аналіз КЗЗ
    - Тестування функцій КЗЗ
    - Аналіз можливостей порушення безпеки
    - Аналіз прихованих каналів
- Середовище розробки
  - Інструментальні засоби
  - Засоби керування процесом розроблення
  - Процедура дистрибуції

FCITS – Вимоги до технології розробки

- Документування
  - Документування функцій КЗЗ
  - Повна документація на продукт ІТ (інтерфейси, компоненти, модулі, структура КЗЗ, методика проектування, вихідні тексти і специфікація апаратних засобів)
  - Документування тестування і аналізу продукту ІТ
    - Документування процесу тестування функцій
    - Документування аналізу можливостей порушення безпеки
    - Документування аналізу прихованих каналів
  - Документування середовища і процесу розроблення
- Супроводження
  - Документація користувача
  - Настанова з адміністрування системи безпеки
  - Процедура оновлення версій і виправлення помилок
  - Процедура інсталяції

FCITS – Вимоги до процесу кваліфікаційного аналізу

- Аналіз
  - Аналіз архітектури
  - Аналіз реалізації
- Контроль
  - Контроль середовища розроблення
  - Контроль процесу супроводження продукту ІТ
- Тестування
  - Тестування функцій КЗЗ виробником
  - Незалежне тестування функцій КЗЗ

FCITS – Висновки

- Вперше запропонована концепція профілю захисту
- У стандарті визначені три незалежні групи вимог
- Функціональні вимоги безпеки добре структуровані
- Вимоги до технології розроблення змушують виробників застосовувати сучасні технології програмування, що дозволяють підтвердити безпеку продукту
- Вимоги до процесу кваліфікаційного аналізу узагальнені і не містять конкретних методик
- Відсутня загальна оцінка рівня безпеки за допомогою універсальної шкали, запропоновано незалежне ранжирування вимог кожної групи