Управление требованиями и проектирование информационных систем

Лекция 15

Старичков Н.Ю., ВШЭ ВШБ ДБИ, 1 модуль 2021/2022 уч.года

Информационная безопасность

Виды требований информационной безопасности

- **Функциональные требования** - предъявляемые требования к функциям безопасности, реализующим их механизмам, требования качества других механизмов ИС
- **Требования доверия** - пассивный аспект защиты; требования, предъявляемые к технологии и процессу разработки и эксплуатации ИС

Угрозы информационной безопасности

Угроза характеризуется:

- Источник угрозы
- Метод воздействия
- Уязвимости, которые могут быть использованы
- Ресурсы (в т.ч. и данные), которые могут пострадать

Функциональные требования

Классы требований

- Идентификация и аутентификация
- Защита данных пользователя
- Защита функций безопасности
- Управление безопасностью
- Аудит безопасности
- Доступ к объекту оценки
- Приватность
- Использование ресурсов
- Криптографическое обеспечение
- Связь
- Доверенный маршрут (для связи с сервисами безопасности)

Требования доверия безопасности

Классы требований

- Требования к разработке системы
- Поддержка жизненного цикла
- Тестирование
- Оценка уязвимостей
- Поставка и эксплуатация
- Управление конфигурацией
- Требования к документации по использованию
- Поддержка доверия
- Оценка профиля защиты
- Оценка задания на безопасность

Атака - основные понятия

- **Атака** - любое действие, использующее уязвимость системы и приводящее к нарушению политики безопасности
- **Механизм безопасности** - программное и/или аппаратное средство, которое определяет и/или предотвращает атаку
- **Сервис безопасности** - сервис, который обеспечивает заданный уровень безопасности, либо определяет осуществление атаки. *Сервис безопасности* использует один или несколько *механизмов безопасности*

Классификация атак

- **По месту возникновения:**
  - Локальные атаки
  - Удаленные атаки
- **По воздействию на ИС:**
  - Активные атаки (нарушают функционирование)
  - Пассивные атаки (не нарушают функционирование)

Пассивная сетевая атака

У атакующего:

- Нет возможности модифицировать передаваемое сообщение
- Нет возможности отправить свое сообщение

Активные сетевые атаки

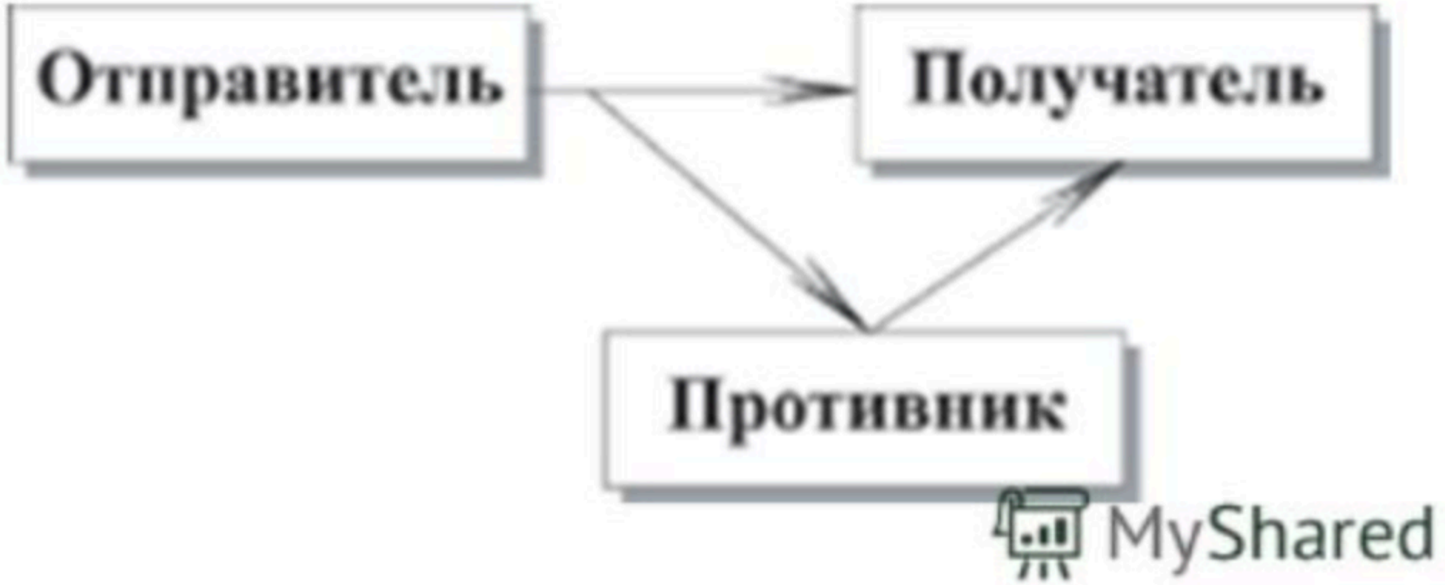
- **Отказ в обслуживании** (DoS - Denial of Service)
  - **DDoS** - Distributed Denial of Service
- **Модификация потока данных** (Man in the Middle)

Активные сетевые атаки

- **Создание ложного потока** (фальсификация)

Активные сетевые атаки

- **Повторное использование** (replay-атака)



MyShared

Сервисы безопасности

- Идентификация и аутентификация
- Управлние доступом
- Протоколирование и аудит
- Шифрование
- Контроль целостности
- Экранирование
- Анализ защищенности
- Обеспечение отказоустойчивости
- Обеспечение безопасного восстановления

Классификация мер безопасности

- Превентивные
- Меры обнаружения нарушений
- Локализующие зону воздействия
- Меры по выявлению нарушений
- Меры восстановления режима безопасности

Аутентификация и авторизация

Ликбез

- Пароли и пин-коды
- Специальные устройства (например, USB-брелки, смарткарты и т.п.)
- Биометрия
- Двухфакторная аутентификация (смс / звонок и т.п.)

С чем будете постоянно сталкиваться?

Ликбез

- **Двухфакторная аутентификация**
- **VPN** - Virtual Private Network
- **Цифровая подпись** - обычная и усиленная
- **Шифрование переписок** - ассиметричное

Отражение безопасности в требованиях

- Требования к архитектуре
- Требования к инструментам и языкам программирования
- Требования к рабочему проекту и разработке ПО
- Требования к кодированию
- Требования к тестированию (в т.ч. интеграционному)

Основные принципы безопасности ИС

- **Безопасность**
  - Должна соответствовать роли и целям организации
  - Требует комплексного и целостного подхода
  - Должна быть неотъемлемой частью системы
  - Должна быть экономически оправданной
  - Должна проходить аудит
- Ответственность должна быть четко определена
- Важную роль имеют административные и социальные факторы

tbc…