Технологии и продукты Microsoft в обеспечении ИБ

Лекция 2. Моделирование угроз ИБ: различные подходы

Цели

- Рассмотреть методы и инструменты анализа и контроля информационных рисков
- Изучить преимущества и недостатки Количественная оценка соотношения потерь от угроз безопасности и затрат на создание системы защиты
- Провести сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, Гексада Паркера, 5A, STRIDE
- Обосновать выбор модели STRIDE как основы для изложения материалов курса

Оценка рисков безопасности

- Оценка может осуществляться на основе количественных и качественных шкал
- Примерами методик оценки рисков являются NIST-800, OCTAVE, CRAMM, Методика оценки РС БР ИББС – 2.3 (проект) и т.д.
- Методика предполагает разработку модели угроз для информационных активов, определенных в рамках проекта

Качественная шкала оценки ущерба

1. **Малый ущерб**
   Приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании
2. **Умеренный ущерб**
   Вызывает заметные потери материальных активов или к умеренному влиянию на репутацию компании
3. **Ущерб средней тяжести**
   Приводит к существенным потерям материальных активов или значительному урону репутации компании
4. **Большой ущерб**
   Вызывает большие потери материальных активов или наносит большой урон репутации компании
5. **Критический ущерб**
   Приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке

Качественная оценка вероятности проведения атаки

1. **Очень низкая**
   Атака практически никогда не будет проведена.
   Уровень соответствует числовому интервалу вероятности **[0, 0.25)**

2. **Низкая**
   Вероятность проведения атаки достаточно низкая.
   Уровень соответствует числовому интервалу вероятности **[0.25, 0.5)**

3. **Средняя**
   Вероятность проведения атаки приблизительно равна **0,5**

4. **Высокая**
   Атака, скорее всего, будет проведена.
   Уровень соответствует числовому интервалу вероятности **(0.5, 0.75]**

5. **Очень высокая**
   Атака почти наверняка будет проведена.
   Уровень соответствует числовому интервалу вероятности **(0.75, 1]**

Пример таблицы определения уровня риска информационной безопасности

Вероятность атаки / Ущерб	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Малый ущерб	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Умеренный ущерб	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Средний ущерб	Низкий риск	Средний риск	Средний риск	Высокий риск	Высокий риск
Большой ущерб	Средний риск	Средний риск	Высокий риск	Высокий риск	Высокий риск
Критический ущерб	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Определение допустимого уровня риска

Вероятность атаки / Ущерб	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Малый ущерб	Допусти-мый риск	Допусти-мый риск	Допусти-мый риск	Допусти-мый риск	Допусти-мый риск
Умеренный ущерб	Допусти-мый риск	Допусти-мый риск	Допусти-мый риск	Допусти-мый риск	Недопусти-мый риск
Средний ущерб	Допусти-мый риск	Допусти-мый риск	Допусти-мый риск	Недопусти-мый риск	Недопусти-мый риск
Большой ущерб	Допусти-мый риск	Допусти-мый риск	Недопусти-мый риск	Недопусти-мый риск	Недопусти-мый риск
Критический ущерб	Средний риск	Недопусти-мый риск	Недопусти-мый риск	Недопусти-мый риск	Недопусти-мый риск

Количественная оценка рисков

Количественная шкала оценки вероятности проведения атаки

Вероятность проведения атаки измеряется от 0 до 1

Количественная шкала оценки уровня ущерба

Ущерб измеряется в финансовом эквиваленте (в денежном выражении)

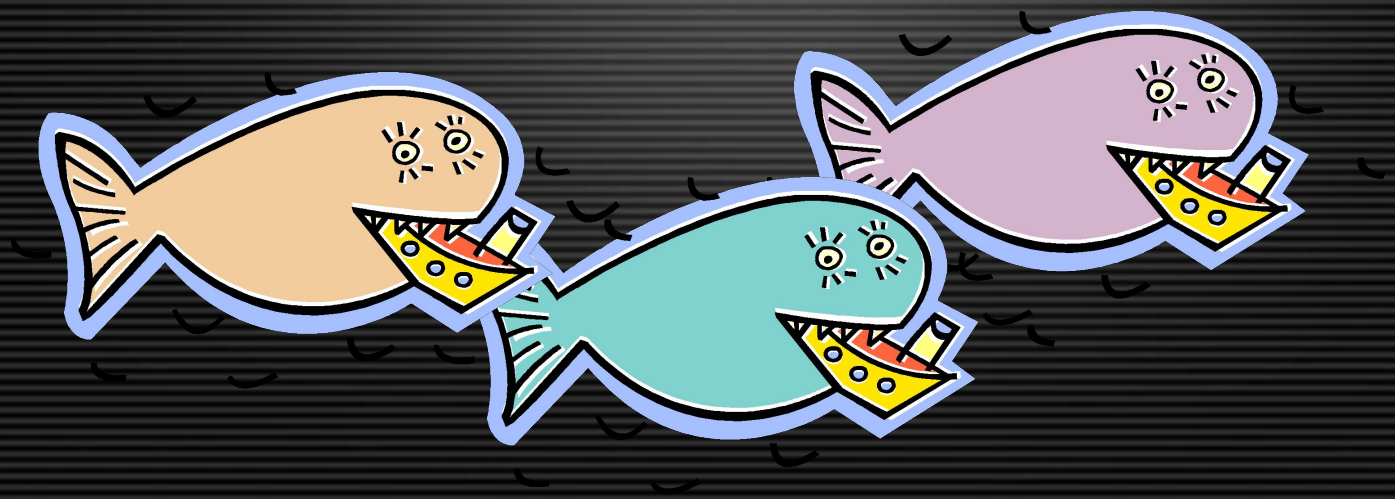
РИСК = Вероятность угрозы X Ущерб

Анализ рисков

- Определение приемлемого уровня риска
- Выбор защитных мер, позволяющих минимизировать риски до приемлемого уровня
- Варианты управления рисками безопасности
  - уменьшение риска за счёт использования дополнительных организационных и технических средств защиты
  - уклонение от риска путём изменения архитектуры или схемы информационных потоков АС
  - изменение характера риска, например, в результате принятия мер по страхованию
  - принятие риска в том случае, если он уменьшен до того уровня, на котором он не представляет опасности для АС

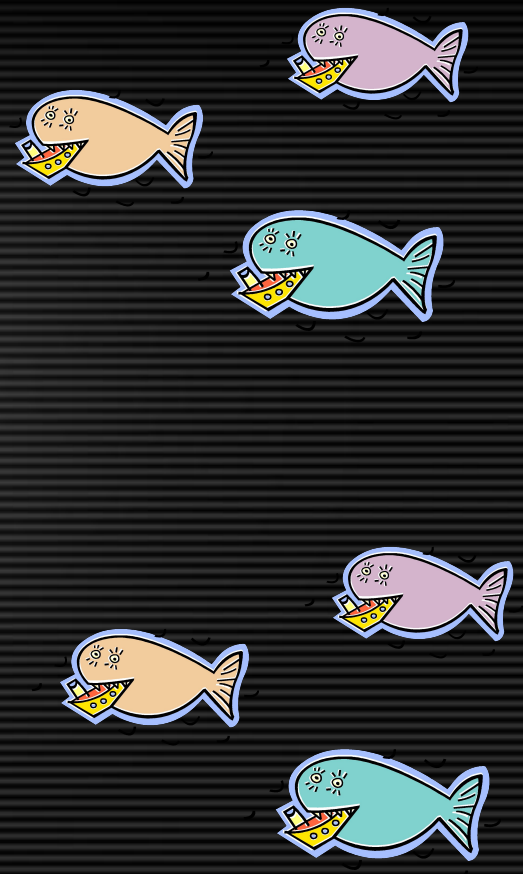
3 кита информационной безопасности

1. Конфиденциальность
2. Целостность
3. Доступность



Гексада Паркера

1. Конфиденциальность
2. Целостность
3. Доступность
4. Управляемость
5. Подлинность
6. Полезность



5A

- **Authentication** (аутентификация: кто ты?)
- **Authorization** (авторизация: что тебе можно делать?)
- **Availability** (доступность: можно ли получить работать с данными?)
- **Authenticity** (подлинность: не повреждены ли данные злоумышленником?)
- **Admissibility** (допустимость: являются ли данные достоверными, актуальными и полезными?)

Модель угроз информационной безопасности STRIDE

Spoofing
Притворство

Tampering
Изменение

Repudiation
Отказ от ответственности

Information Disclosure
Утечка данных

Denial of Service
Отказ в обслуживании

Elevation of Privilege
Захват привилегий

Использованные источники

- **Сердюк В.А.** Аудит информационной безопасности – основа эффективной защиты предприятия // "BYTE/Россия", 2006 №4(92), стр. 32-35
- **Медведев И.** Моделирование угроз безопасности // Software Engineering Conference (Russia) “Path to Competitive Advantage”, SEC(R) 200
- **Schneier B.** Updating the Traditional Security Model //Schneier on security. Available at: http://www.schneier.com/blog/archives/2006/08/updating_the_tr.html
- **Parker D.** Fighting Computer Crime. New York, NY: John Wiley & Sons, 1998


Спасибо за внимание!
Вопросы?