Информационная безопасность

Угрозы информационной безопасности

(презентация к лекции 6)

Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя [Электронный ресурс]. URL: rv-lab.ru (2017).

Угрозы информационной безопасности

Определения

- **Угроза** – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам
- **Угрозой информационной безопасности** называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или компоненты АИС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений
- **Атака** — попытка реализации угрозы
- **Нарушение** — реализация угрозы

Угрозы информационной безопасности

Виды угроз

По аспекту ИБ
Угрозы конфиденциальности
Угрозы целостности
Угрозы доступности
Угрозы апеллируемости

По источнику угроз
Внешние
Внутренние

По природе возникновения
Естественные угрозы
Искусственные угрозы:
- непреднамеренные
- умышленные

По компонентам АИС
Угрозы данным
Угрозы программному обеспечению
Угрозы аппаратному обеспечению
Угрозы поддерживающей инфраструктуре

Модель категоризации угроз STRIDE

Корпорация Microsoft

Spoofing (подмена данных) – может ли кто-то или что-то обмануть механизмы *аутентификации*
Tampering (изменение данных) – нарушение *целостности*
Repudiation (аннулирование) – может ли пользователь отрицать совершенные им нелегальные действия; нарушение *апеллируемости*
Information Disclosure (раскрытие информации) – нарушение *конфиденциальности*.
Denial of Service (отказ в обслуживании) – нарушение *доступности*.
Elevation of privilege (повышение прав доступа) – нарушение процедуры *авторизации*

Оценка угроз информационной безопасности

Мера риска $R = P \cdot C$

P – вероятность наступления нежелательного события

C – ущерб от наступления такого события

Реализуемость угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Методика оценки угроз DREAD

Корпорация Microsoft

Damage – опасность.
Reproducibility – воспроизводимость.
Exploitability – легкость использования уязвимости.
Affected users – число затронутых пользователей.
Discoverability – легкость обнаружения уязвимости.
Risk = (D + R + E + A + D) / 5.

Модель угроз

Модель угроз информационной безопасности – это описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштаба потенциального ущерба.

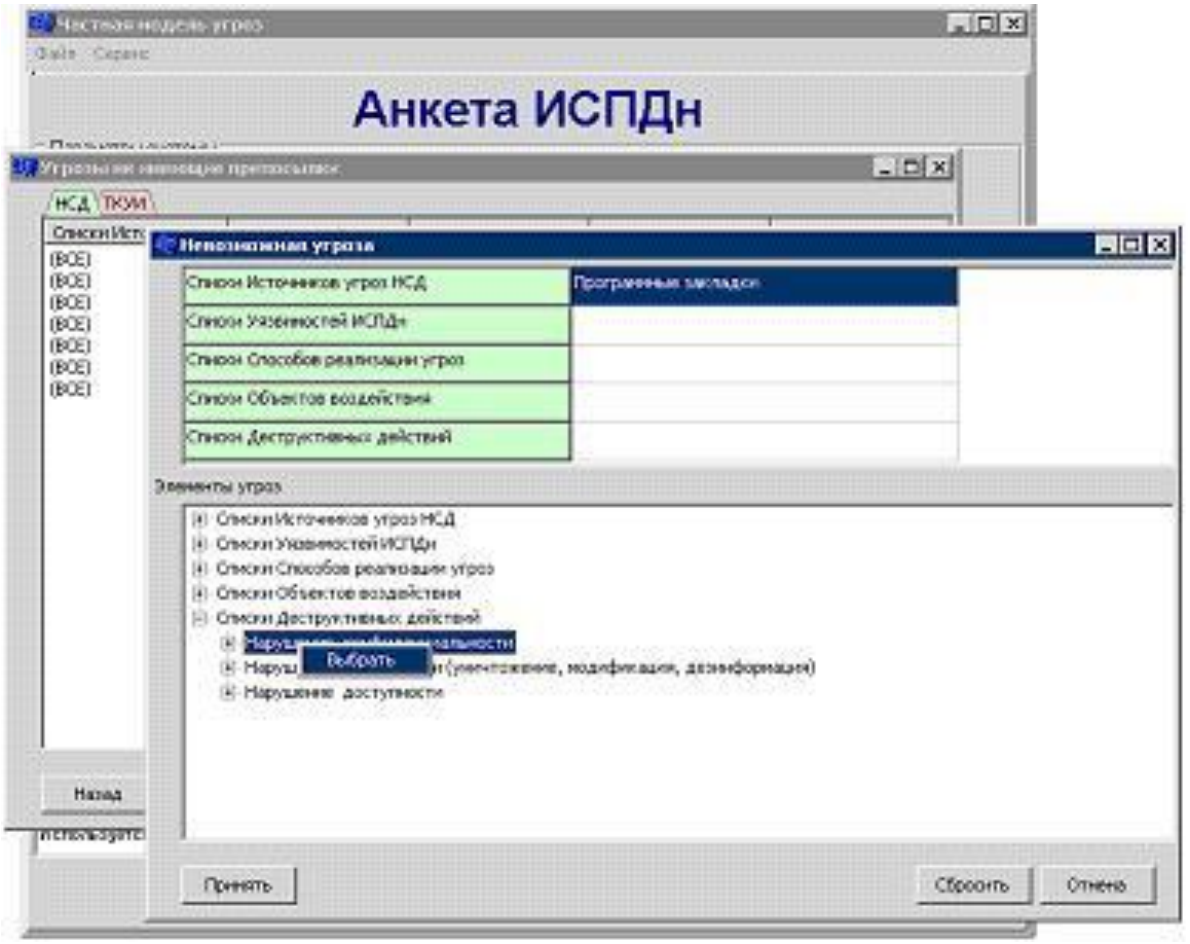
Этапы построения модели угроз

1. Выявить критические объекты информационной системы.
2. Выявить источники угроз (человек, материальные объекты, физические явления).
3. Для каждого критического объекта построить перечень возможных угроз, выявить способы их реализации, оценить реализуемость (низкая, средняя, высокая или очень высокая).
4. Провести оценку материального ущерба и других возможных последствий угроз. Выявить актуальные угрозы.

При разработке системы безопасности необходимо предусмотреть *меры противодействия* каждой из актуальных угроз (таким образом, чтобы эти угрозы перешли в разряд неактуальных из-за низкой реализуемости).

Программные средства построения модели угроз

Программа «Wingdoc ПД» создает документ «Модель угроз персональных данных системы» на основе заполнения анкеты из стандартных вопросов



Модель нарушителя ИБ

Нарушитель информационной безопасности — физическое лицо, случайно или преднамеренно совершающий действия, следствием которых является нарушение информационной безопасности (конфиденциальности, целостности или доступности информации).

Злоумышленник — нарушитель, совершающий попытку выполнения запрещенных операций с данными намеренно и из корыстного интереса

Модель нарушителя информационной безопасности – описание профилей потенциальных нарушителей, включающие их знания, возможности, мотивы и прочие характеристики, важные для оценки соответствующих угроз.

Состав модели нарушителя ИБ

1. Категория лиц:

- Внешние нарушители.
- Внутренние нарушители

2. Мотивы :

- безответственность;
- самоутверждение;
- корыстный интерес.

3. Уровень знаний:

- пользователь;
- администратор;
- программист;
- специалист в области информационной безопасности.

4. Возможности нарушителя :

- сведения от других лиц;
- штатные средства доступа;
- пассивный перехват;
- активный перехват.

5. Время действия:

- во время функционирования АИС;
- во время простоя АИС;
- в любое время.

6. Место действия:

- без доступа на территорию;
- с доступом на территорию;
- с рабочих мест пользователей;
- с доступом к базам данных АИС;
- с доступом к подсистеме защиты.