Тема 2

Угрозы и модель нарушителя информационной безопасности

Содержание темы

- Понятие угрозы. Классификация угроз.
- Классификация уязвимостей информационных объектов.
- Понятие риска. Способы оценки рисков.
- Понятие атаки.
- Модель нарушителя информационной безопасности.
- Статьи Уголовного кодекса Республики Беларусь по вопросам информационной безопасности.

Понятие угрозы

Угроза безопасности объекта – возможное воздействие на объект, которое прямо или косвенно может нанести ущерб его безопасности.

Угроза – это опасность причинения ущерба. Устанавливается жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Например:

- моральный и материальный ущерб деловой репутации организации;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

и т. п.

Классификация угроз

Угрозами безопасности информации являются нарушения при обеспечении:

- **конфиденциальности**;
- **доступности**;
- **целостности**.

Конфиденциальность информации – это свойство информации быть известной только аутентифицированным законным ее владельцам или пользователям.

Нарушения при обеспечении конфиденциальности:

- **хищение** (копирование) информации и средств ее обработки;
- **утрата** (неумышленная потеря, утечка) информации и средств ее обработки.

Классификация угроз

Доступность информации – это свойство информации быть доступной для аутентифицированных законных ее владельцев или пользователей.

Нарушения при обеспечении доступности:

- **блокирование** информации;
- **уничтожение** информации и средств ее обработки.

Классификация угроз

Целостность информации – это свойство информации быть неизменной в семантическом смысле при воздействии на нее случайных или преднамеренных искажений или разрушающих воздействий.

Нарушения при обеспечении целостности:

- **модификация** (искажение) информации;
- **отрицание подлинности** информации;
- **навязывание ложной** информации.

Классификация угроз

Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Все источники угроз безопасности информации можно разделить на три основные группы:

- обусловленные действиями субъекта (**антропогенные**);
- обусловленные техническими средствами (**техногенные**);
- обусловленные стихийными источниками (**стихийные**).

Источники угроз могут находиться как внутри защищаемой организации – **внутренние** источники, так и вне ее – **внешние** источники.

Классификация угроз

Внешние антропогенные источники угроз

Криминальные структуры
Потенциальные преступники и хакеры
Недобросовестные партнеры
Технический персонал поставщиков телекоммуникационных услуг
Представители надзорных организаций и аварийных служб
Представители силовых структур

Классификация угроз

Внутренние антропогенные источники угроз

Основной персонал (пользователи, программисты, разработчики)
Представители службы защиты информации (администраторы)
Вспомогательный персонал (уборщики, охрана)
Технический персонал (жизнеобеспечение, эксплуатация)

Классификация угроз

Внешние техногенные источники угроз

Средства связи
Сети инженерных коммуникации (водоснабжения, канализации)
Транспорт

Классификация угроз

Внутренние техногенные источники угроз

Некачественные технические средства обработки информации
Некачественные программные средства обработки информации
Вспомогательные средства (охраны, сигнализации, телефонии)
Другие технические средства, применяемые в учреждении

Классификация угроз

Внешние стихийные источники угроз

Пожары
Землетрясения
Наводнения
Ураганы
Магнитные бури
Радиоактивное излучение
Различные непредвиденные обстоятельства
Необъяснимые явления
Другие форс-мажорные обстоятельства

Классификация угроз

Все источники угроз имеют разную степень опасности, которую можно количественно оценить, проведя их ранжирование.

Оценка степени опасности проводится по косвенным показателям:

Критерий 1 (K_1):

возможность возникновения источника – определяет степень доступности к возможности использовать уязвимость для антропогенных источников, удаленность от уязвимости для техногенных источников или особенности обстановки для случайных источников.

Классификация угроз

Критерий 2 (K_2):

готовность источника – определяет степень квалификации и привлекательность совершения деяний со стороны источника угрозы для антропогенных источников или наличие необходимых условий для техногенных и стихийных источников.

Критерий 3 (K_3):

фатальность – определяет степень неустранимости последствий реализации угрозы.

Классификация угроз

Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе: 1 – самая минимальная степень влияния оцениваемого показателя на опасность использования источника, а 10 – максимальная.

$$K_{опуг} = \frac{K_1 \cdot K_2 \cdot K_3}{1000}.$$

Уязвимости информационных объектов

Уязвимость объекта – это присущие объекту причины, приводящие к нарушению безопасности информации на объекте.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

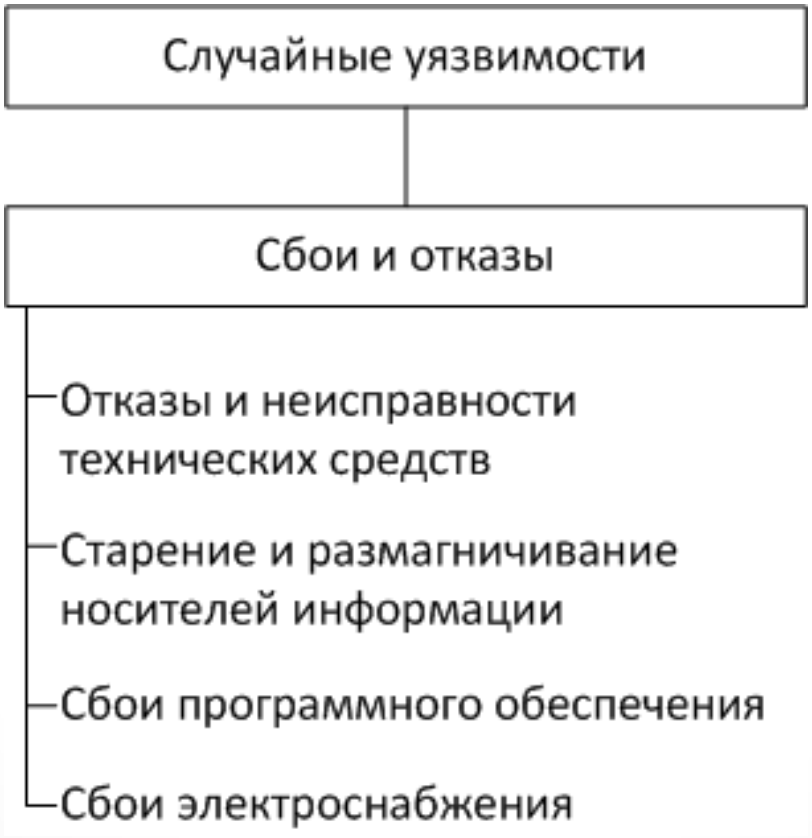
Уязвимости безопасности информации подразделяются на:

- **объективные** (зависят от оборудования);
- **субъективные** (зависят от действий сотрудников);
- **случайные** (зависят от окружающей среды и пр.).

Классификация уязвимостей

Классификация уязвимостей

Классификация уязвимостей



Классификация уязвимостей

Все уязвимости имеют разную степень опасности, которую можно количественно оценить, проведя их ранжирование.

Оценка степени опасности проводится по косвенным показателям:

Критерий 4 (K_4):

фатальность – определяет степень влияния уязвимости на неустранимость последствий реализации угрозы.

Критерий 5 (K_5):

доступность – определяет возможность использования уязвимости источником угроз.

Классификация уязвимостей

Критерий 6 (K_6):

количество – определяет количество элементов объекта, которым характерен та или иная уязвимость.

Каждый показатель оценивается экспертно-аналитическим методом по пятибалльной системе: 1 – самая минимальная степень влияния оцениваемого показателя на опасность использования источника, а 10 – максимальная.

$$K_{опуяз} = \frac{K_4 \cdot K_5 \cdot K_6}{1000}.$$

Риски нарушения безопасности

Риск нарушения безопасности – это возможность реализации угрозы, которая нанесет ущерб владельцу.

Под риском также понимают сочетание вероятности события и его последствий.

Существует **количественная** и **качественная** оценка рисков.

Риски нарушения безопасности

Суть **количественной** оценки рисков сводится к поиску единственного оптимального решения по организации защиты информации из множества существующих.

К количественным методикам управления рисками относятся такие методики, как:

- **CRAMM** (CCTA Risk Analysis and Management Method) и т. п.

Риски нарушения безопасности

Суть **качественной** оценки рисков сводится к проведению общей и частных оценок, позволяющих выработать обоснованное решение о необходимости защиты информации с оценкой предстоящих расходов на эту защиту.

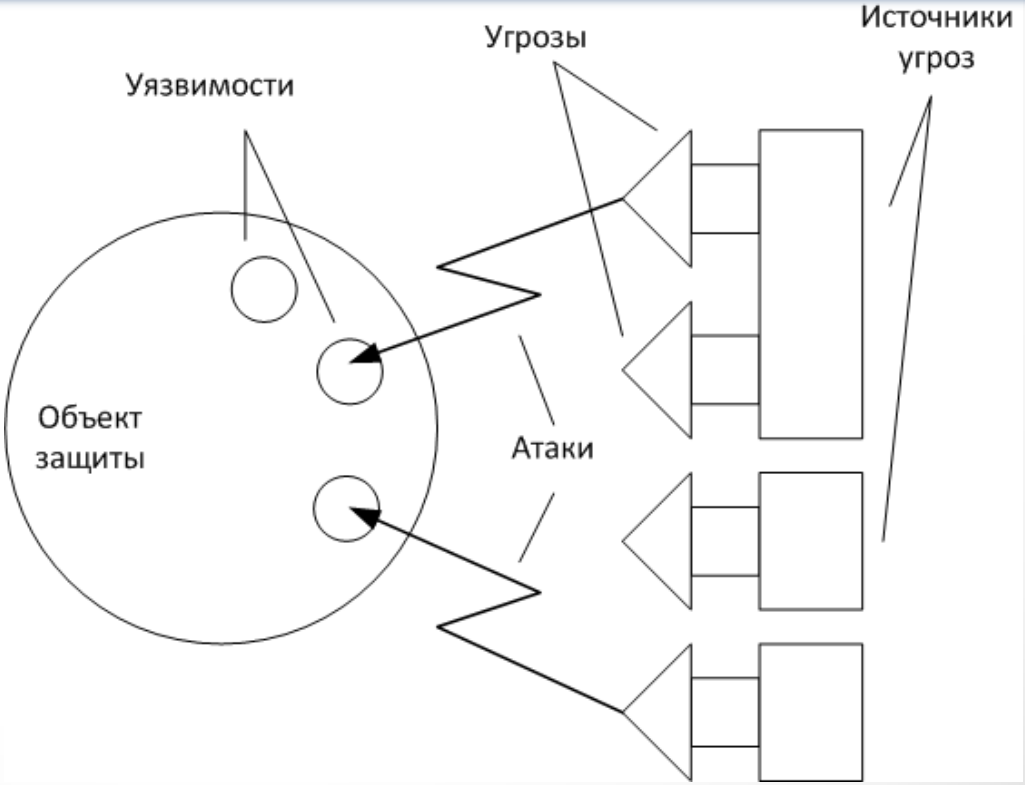
К качественным методикам управления рисками относятся такие методики и соответствующие программные продукты, как:

- **MSAT** (Microsoft Security Assessment Tool) и т. п.

Атака

Атака – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости.

Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая к ущербу.



Модель нарушителя

Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д.

Правильно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности.

Опираясь на построенную модель, уже можно строить адекватную систему информационной защиты!

Модель нарушителя

Чаще всего строится **неформальная** модель нарушителя, отражающая:

- причины и мотивы действий;
- возможности;
- априорные знания;
- преследуемые цели, их приоритетность для нарушителя;
- основные пути достижения поставленных целей;
- способы реализации исходящих от него угроз;
- место и характер действия;
- возможную тактику и т. п.

Нарушители бывают внутренними и внешними по отношению к объекту защиты.

Модель нарушителя

Среди внутренних нарушителей в первую очередь выделяют:

- непосредственных пользователей и операторов информационной системы, в том числе руководителей различных уровней;
- администраторов вычислительных сетей и информационной безопасности;
- прикладных и системных программистов;
- сотрудников службы безопасности;
- технический персонал по обслуживанию зданий и вычислительной техники, от уборщицы до сервисного инженера;
- вспомогательный персонал и временных работников.

Модель нарушителя

Модель нарушителя: конкуренты

Вычислительная мощность технических средств	Мощные вычислительные сети
Доступ к интернету, тип каналов доступа	Собственные каналы с высокой пропускной способностью
Финансовые возможности	Большие возможности
Уровень знаний в области IT	Высокий
Используемые технологии	Современные методы проникновения в информационные системы и воздействия на потоки данных в ней
Знания о построении системы защиты объекта	Могут предпринимать усилия для получения представления о принципах функционирования системы защиты, внедрять своего представителя в службу безопасности
Преследуемые цели	Блокировка функционирования системы, подрыв имиджа, разорение
Характер действий	Скрытый или открытый демонстративный
Глубина проникновения	До победного конца

Уголовный Кодекс Республики Беларусь

Статья 212. Хищение путем использования компьютерной техники

1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации – наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. …

3. …

4. …

Уголовный Кодекс Республики Беларусь

Глава 31. Преступления против информационной безопасности

Статья 349. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, – наказывается штрафом или арестом.

2. …

3. …

Уголовный Кодекс Республики Беларусь

Статья 350. Модификация компьютерной информации

1. Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) – наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. …

Уголовный Кодекс Республики Беларусь

Статья 351. Компьютерный саботаж

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) – наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

2. …

Уголовный Кодекс Республики Беларусь

Статья 352. Неправомерное завладение компьютерной информацией

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, – наказываются общественными работами, или штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Уголовный Кодекс Республики Беларусь

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети – наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет.

Уголовный Кодекс Республики Беларусь

Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами – наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. …

Уголовный Кодекс Республики Беларусь

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, – наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

2. …

3. …