Тема

Угрозы 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.

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.).

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.

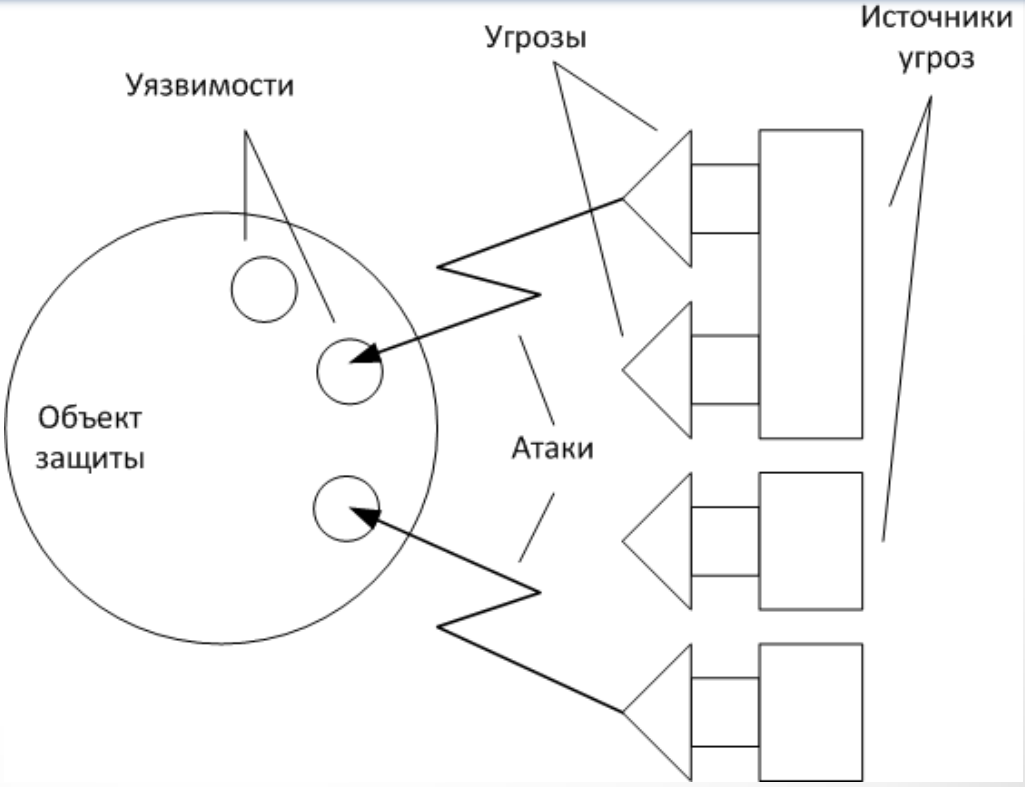
К качественным методикам управления рисками относятся такие методики и соответствующие программные продукты, как:

- **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