ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное образовательное учреждение г. Москвы Колледж связи № 54 им. П.М.Вострухина

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

"БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ"

РАЗДЕЛ I. Основы безопасности информационных технологий Тема 3. Угрозы безопасности информационных технологий

МОСКВА 2016

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Важнейший аспект проблемы обеспечения безопасности компьютерных систем – определение, анализ и классификация возможных угроз безопасности автоматизированных систем.

Перечень значимых угроз, оценки вероятностей их реализации, а также **модель нарушителя** – основа для проведения анализа рисков и формирования требований к системе защиты автоматизированной системы.

Лаборатория Информационной Безопасности

Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем

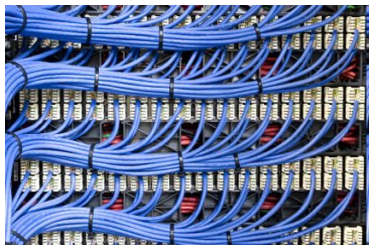
Наиболее доступны!

Рабочие станции

Структурно-функциональные элементы автоматизированной системы

Сетевые устройства
(маршрутизаторы, коммутаторы, шлюзы)

Сервера или host-машины

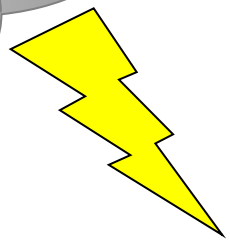


Каналы связи
(локальные, телефонные, и т.д.)

Лаборатория Информационной Безопасности

Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений

Потенциально возможное событие, вызванное некоторым действием, процессом или явлением, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов



НАРУШЕНИЕ (АТАКА) – реализация угрозы безопасности(наступление соответствующего события)

УГРОЗА интересам субъектов информа-ционных отношений

Лаборатория Информационной Безопасности

Типы угроз безопасности ГОСТ Р 50922-96

Угрозы безопасности

Утечка информации (разглашение, разведка, несанкционированный доступ к информации)

Несанкционированное воздействие на информацию и ее носители – воздействие на информацию с нарушением установленных прав и/или правил на изменение информации

Несанкционированное воздействие на информацию и ее носители

1. Модификация - изменение содержания или объема информации на ее носителях.

Подделка информации – умышленная несанкционированная модификация информации с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.

Уничтожение информации – случайное или умышленное стирание информации на ее носителях.

Искажение информации – преднамеренная (внесение ложных данных) или случайная модификация информации (внешние воздействия (помехи), сбои в работе аппаратуры или неумелые действия обслуживающего персонала.

Лаборатория Информационной Безопасности

Несанкционированное воздействие на информацию

Несанкционированное воздействие на информацию и ее носители

2. Блокирование – утрата доступности, выражающаяся в затруднении или прекращении санкционированного доступа к ней

3. Хищение носителя. Даже если это не привело к утечке информации

4. Утрата носителя. Отличается от хищения непредумышленным характером

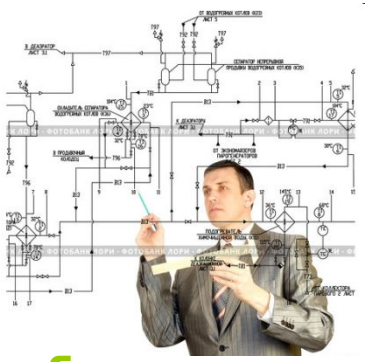
Лаборатория Информационной Безопасности

Источники угроз безопасности

1. Стихийные бедствия

3. Аварии, сбои и отказы оборудования

2. Преднамеренные действия нарушителей и злоумышленников



4. Ошибки проектирования и разработки компонентов АС

5. Ошибки эксплуатации

Лаборатория Информационной Безопасности

Классификация угроз безопасности по природе их возникновения

Угрозы безопасности

- **Естественные (объективные)**
- **Искусственные (субъективные)**
  - **Случайные**
  - **Преднамеренные**

Классификация угроз безопасности по природе их возникновения

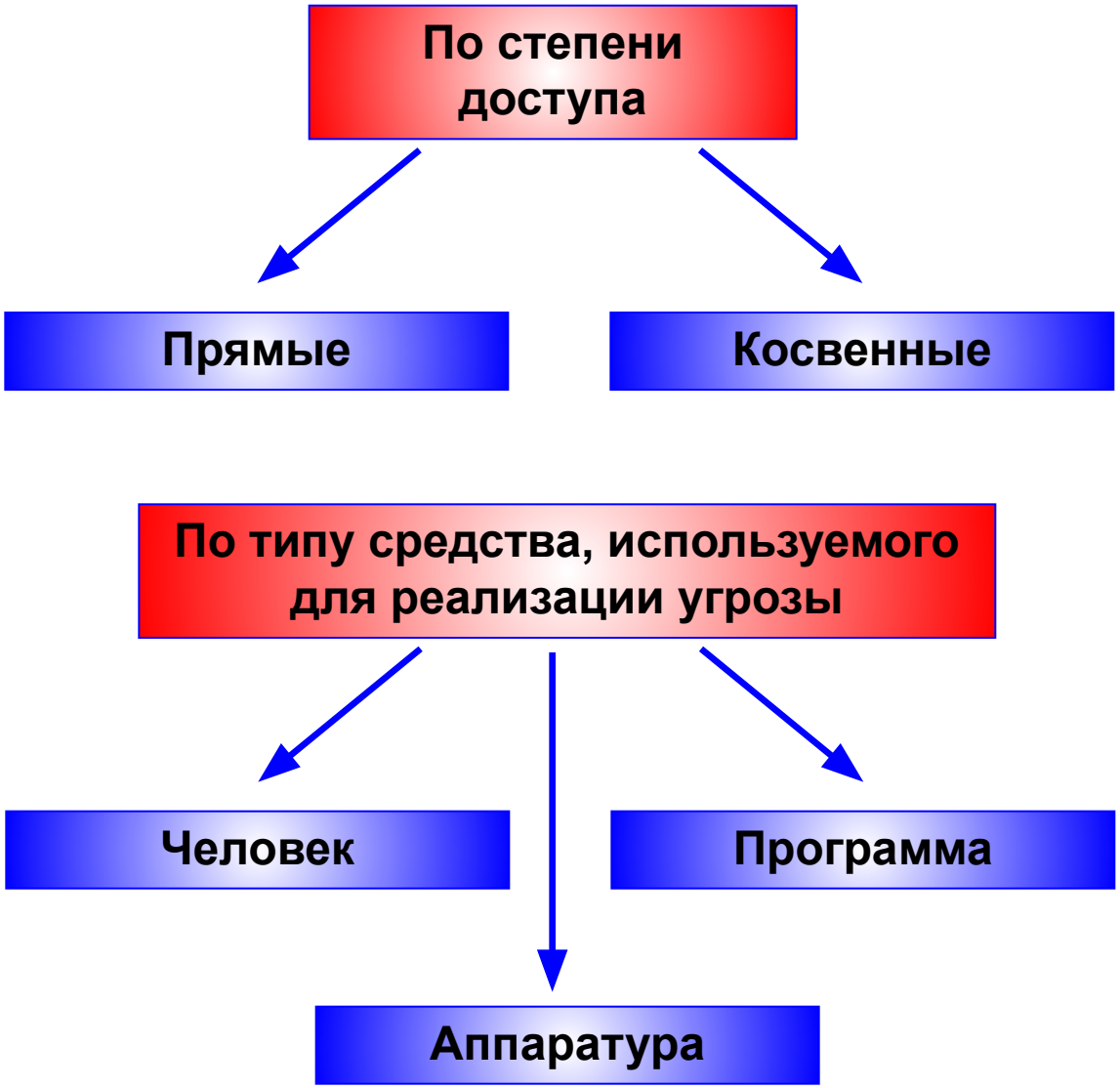
Естественные угрозы – это угрозы, вызванные воздействием на АС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы – это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

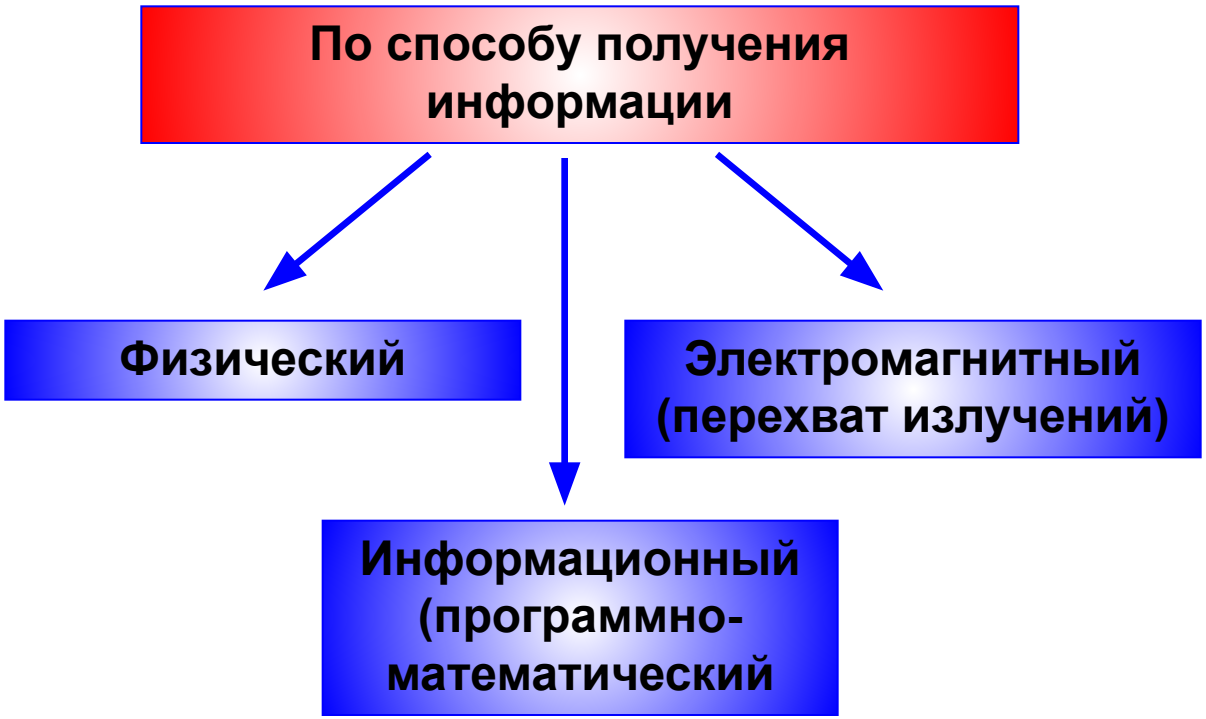
- *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.);

- *преднамеренные* (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Классификация каналов проникновения в автоматизированную систему и утечки информации



Классификация каналов проникновения в автоматизированную систему и утечки информации



Неформальная модель нарушителя

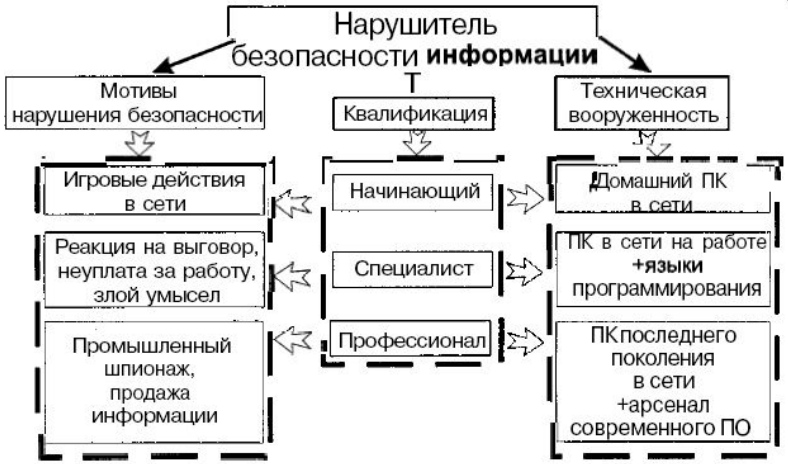


Рис. **1.5.** Модель нарушителя безопасности информации

Нарушитель - лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Модель (образ) нарушителя представляет собой его комплексную характеристику отражающую его возможное психологическое состояние, уровень физической и технической подготовленности, осведомленности, которая позволяет оценить степень его способности в практической реализации проникновения.

Неформальная модель нарушителя

При построении модели нарушителя обычно формулируются **четыре основных предположения**:

1. О категориях лиц, к которым может принадлежать нарушитель.

2. О мотивах действий нарушителя и преследуемых им целях.

3. О квалификации нарушителя и его технической оснащенности.

4. О характере возможных действий нарушителей.

Категории нарушителей

Категории нарушителей

Внутренние

- конечные пользователи (операторы);
- обслуживающий персонал (техники);
- сотрудники отдела разработки и сопровождения ПО;
- сотрудники службы безопасности АС;
- руководители различных уровней.

Внешние

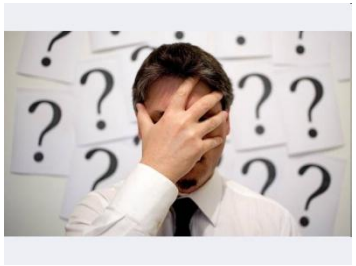
- тех. персонал сторонних организаций;
- клиенты;
- посетители;
- представители взаимодействующих организаций;
- лица, случайно или умышленно нарушившие пропускной режим;
- любые лица за пределами контролируемой территории.

Мотивы совершения нарушений

Месть

Корыстный интерес

Принуждение



Безответственность (некомпетентность, халатность)

Мотивы совершения нарушений

Вандализм

Идейные соображения

Самоутверждение

Лаборатория Информационной Безопасности

Квалификация нарушителя

1. Знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами.

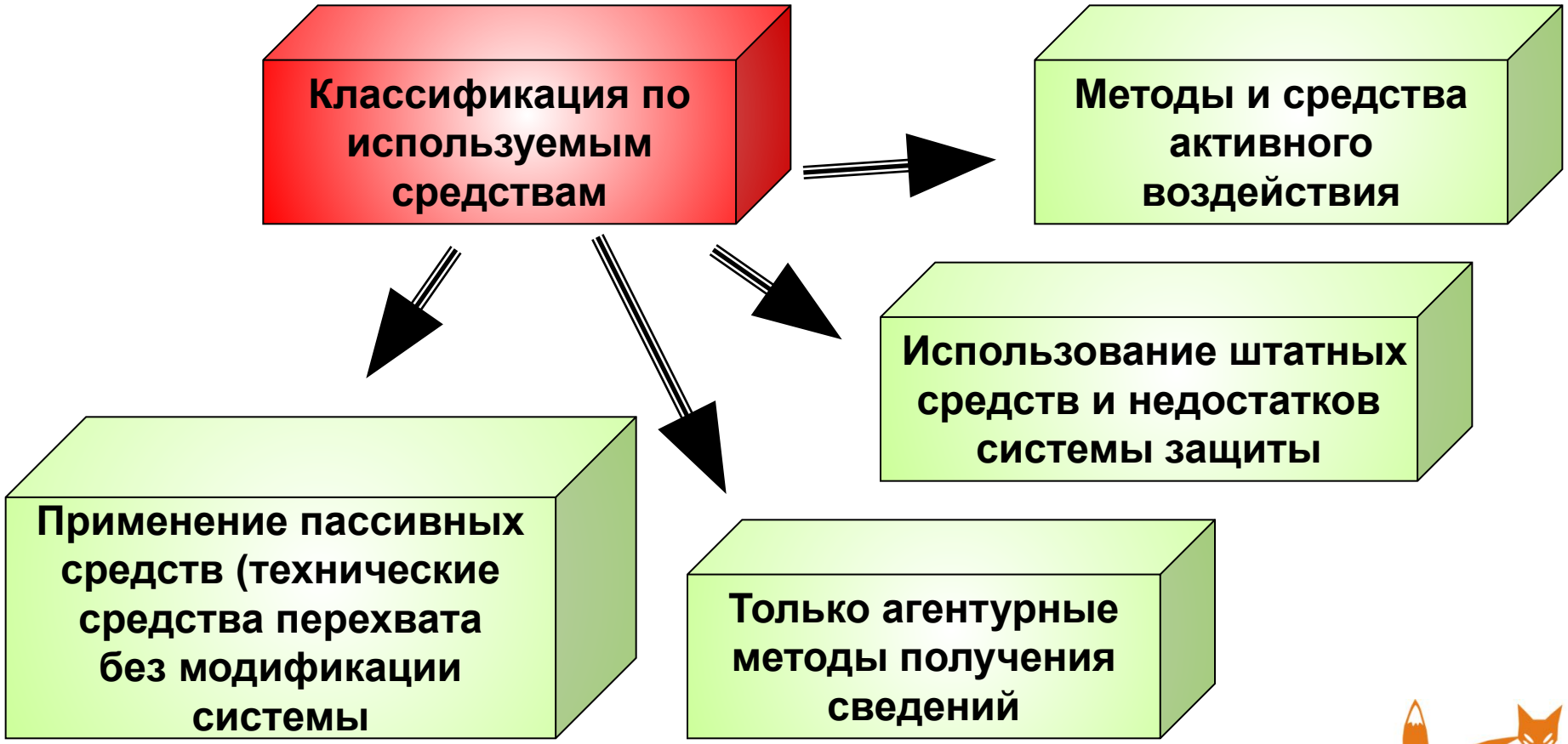
2. Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания.

3. Обладает высоким уровнем знаний в области программирования и ВТ, проектирования и эксплуатации автоматизированных информационных систем.

4. Знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

Лаборатория Информационной Безопасности

Классификация нарушителя по уровню возможностей



Характер возможных действий

Характер возможных действий нарушителя

По месту действия

- без доступа на контролируемую территорию организации;
- с контролируемой территории, но без доступа в здания и сооружения;
- с рабочих мест конечных пользователей;
- с доступом в зону хранилищ данных;
- с доступом в зону управления средствами обеспечения

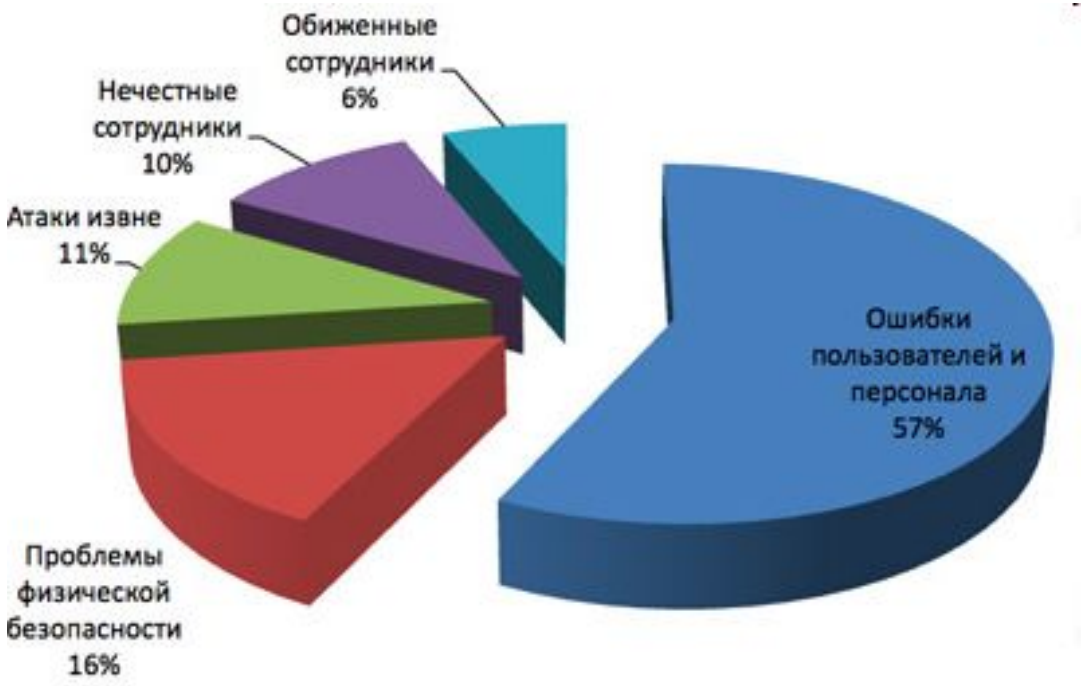
По времени действия

- в процессе функционирования АС (во время работы);
- в период неактивности компонентов системы;
- как в процессе функционирования так и в период неактивности.

Модель нарушителя

Пользователи системы и ее персонал, **с одной стороны**, являются составной частью, **необходимым элементом АС**. **С другой стороны**, они же являются **основным источником угроз** и движущей силой нарушений и преступлений.

Результаты анализа нарушений и проблем с ИТ, проведенного Институтом компьютерной безопасности (Computer Security Institute)



Согласно одному из последних обзоров аналитического подразделения журнала **The Economist**, информационная безопасность является одной из самых приоритетных проблем для **78%** из 254 опрошенных по всему миру первых лиц компаний.

Респонденты признали, что большую часть проблем создают сами сотрудники корпораций. По статистике опроса, источник **83%** проблем с безопасностью находится внутри компании.

Лаборатория Информационной Безопасности

Выводы

1. Уязвимыми являются буквально все основные структурно-функциональные элементы современных распределенных АС: рабочие станции, серверы (Host -машины), и т.д.;

2. Защищать компоненты АС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, и т.п.;

3. Имеется широчайший спектр вариантов (путей) преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией;

4. Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики - важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Контрольные вопросы

Контрольные вопросы:

1. Перечислите структурно-функциональные элементы автоматизированной системы.
2. Дайте определение угрозы интересам субъектов информационных отношений. Что является реализацией угрозы?
3. Назовите типы угроз безопасности согласно ГОСТ Р 50922-96.
4. Какие виды несанкционированного воздействия на информацию и ее носители вы знаете?
5. Что является источниками угроз безопасности АС и информации?
6. Как классифицируются угрозы безопасности АС и информации по природе из возникновения? Раскройте их сущность.
7. Как классифицируются каналы проникновения в автоматизированную систему и каналы утечки информации?
8. Кто такой нарушитель? Что собой представляет модель нарушителя?
9. Какие предположения обычно формулируются при построении модели нарушителя?
10. Какие категории нарушителей вы знаете?
11. Как можно классифицировать характер возможных действий нарушителя?

Лаборатория Информационной Безопасности

Спасибо за внимание!

Лаборатория Информационной Безопасности