

Для проведения анализа уязвимости целесообразно иметь:

модели каналов утечки информации и НСД;
методики определения вероятности информационного контакта;
модель нарушителя;
перечень возможностей информационных атак, вирусов и др.
вредоносных программ;
способы применения и тактико-технические возможности
технических средств используемых для НСД и других
несанкционированных действий с системой;
методику оценки информационной безопасности.

Этапы проведения анализа уязвимости:

1. выбор анализируемых объектов и определение степени детальности их рассмотрения;
2. моделирование каналов утечки информации и НСД, формирование модели нарушителя;
3. оценка потерь (возможного ущерба);
4. определение стратегии управления рисками.

УРОВНИ СИСТЕМЫ

- **Внешний уровень** (сетевые сервисы);
- **Сетевой уровень** (доступ к ресурсам внутри локальных сетей);
- **Системный уровень** (управление доступом к ресурсам ОС);
- **Уровень приложений** (прикладное ПО)

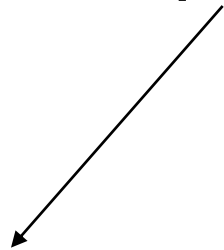
Под *каналом утечки* информации понимается:

физический путь от источника информации, по которому возможна утечка информации к злоумышленнику. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства приема и фиксации информации на стороне злоумышленника.

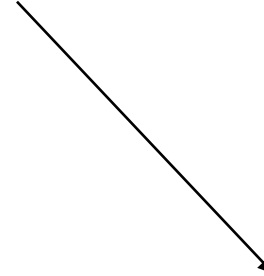
Каналы утечки информации можно разделить на
следующие группы:

- визуально-оптические;
- акустические (включая и акустико-преобразовательные);
- электромагнитные (включая магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида).

МОДЕЛЬ КАНАЛА

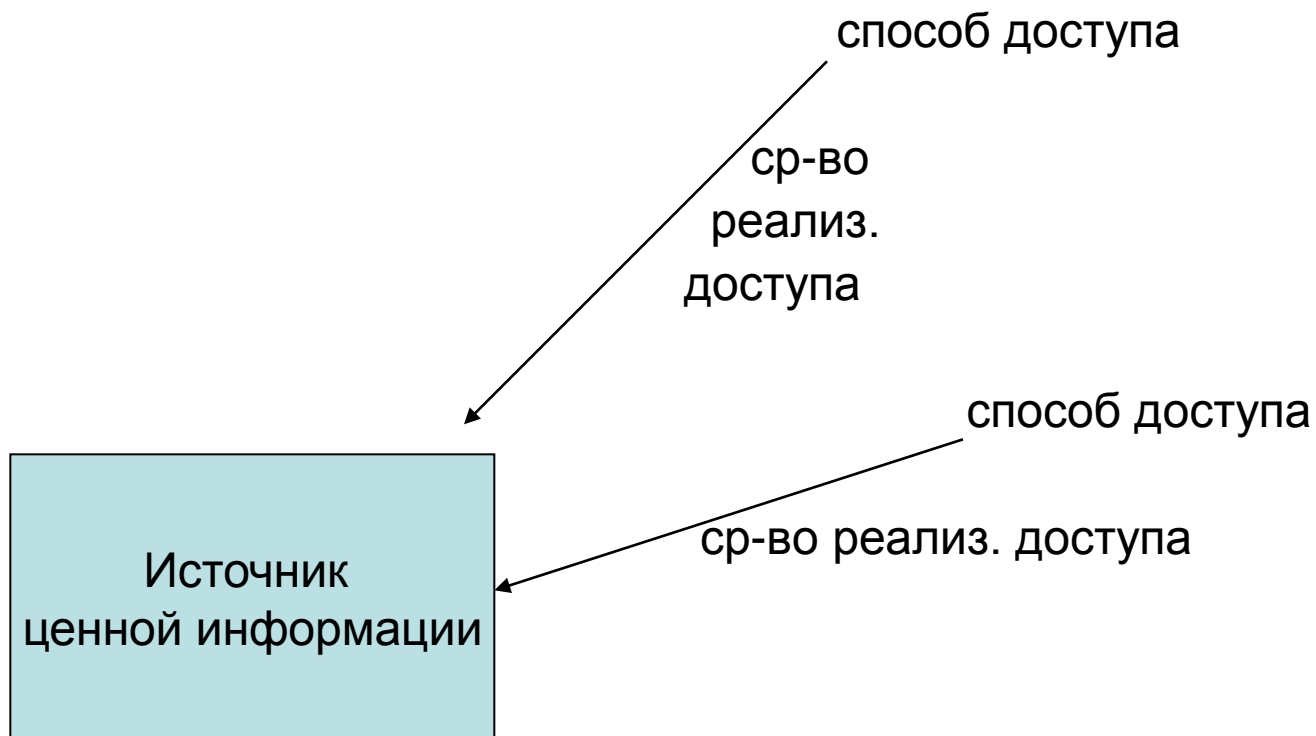


ПУТЬ ИНФ. КОНТАКТА



ВЕРОЯТНОСТЬ
УСТАНОВЛЕНИЯ
ИНФ. КОНТАКТА

ЧАСТНАЯ МОДЕЛЬ ИНФ.КОНТАКТА



облик нарушителя

«Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»

Необходимо определить:

- категорию лиц, к которым может принадлежать нарушитель;
- мотивы действий нарушителя (пре-следуемые нарушителем цели);
- техническую оснащенность и используемые для совершения нарушения методы и средства;
- предполагаемые место и время осуществления незаконных действий на-рушителя;
- ограничения и предположения о ха-рактере возможных действий.

Несколько подходов к управлению рисками

- уменьшение риска
- уклонение от риска
- изменение характера риска
(страхование отдельных рисков);
- принятие риска

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

- модели каналов утечки информации и НСД;
- методики определения вероятностей установления информационного контакта для внешних нарушителей;
- сценарии возможных действий нарушителя по каждому из видов угроз, учитывающие модель нарушителя, возможности системы защиты информации и технических средств разведки, а также действия нарушителя после ознакомления с информацией, ее искажения или уничтожения.