Особенности обеспечения безопасности предприятий почтовой связи

Лекция 2.
Основные угрозы безопасности предприятия.

- Учебные вопросы:
- 1. Модель угроз безопасности предприятия.
- 2. Модель нарушителя безопасности предприятия.

Модель угроз предприятию связи

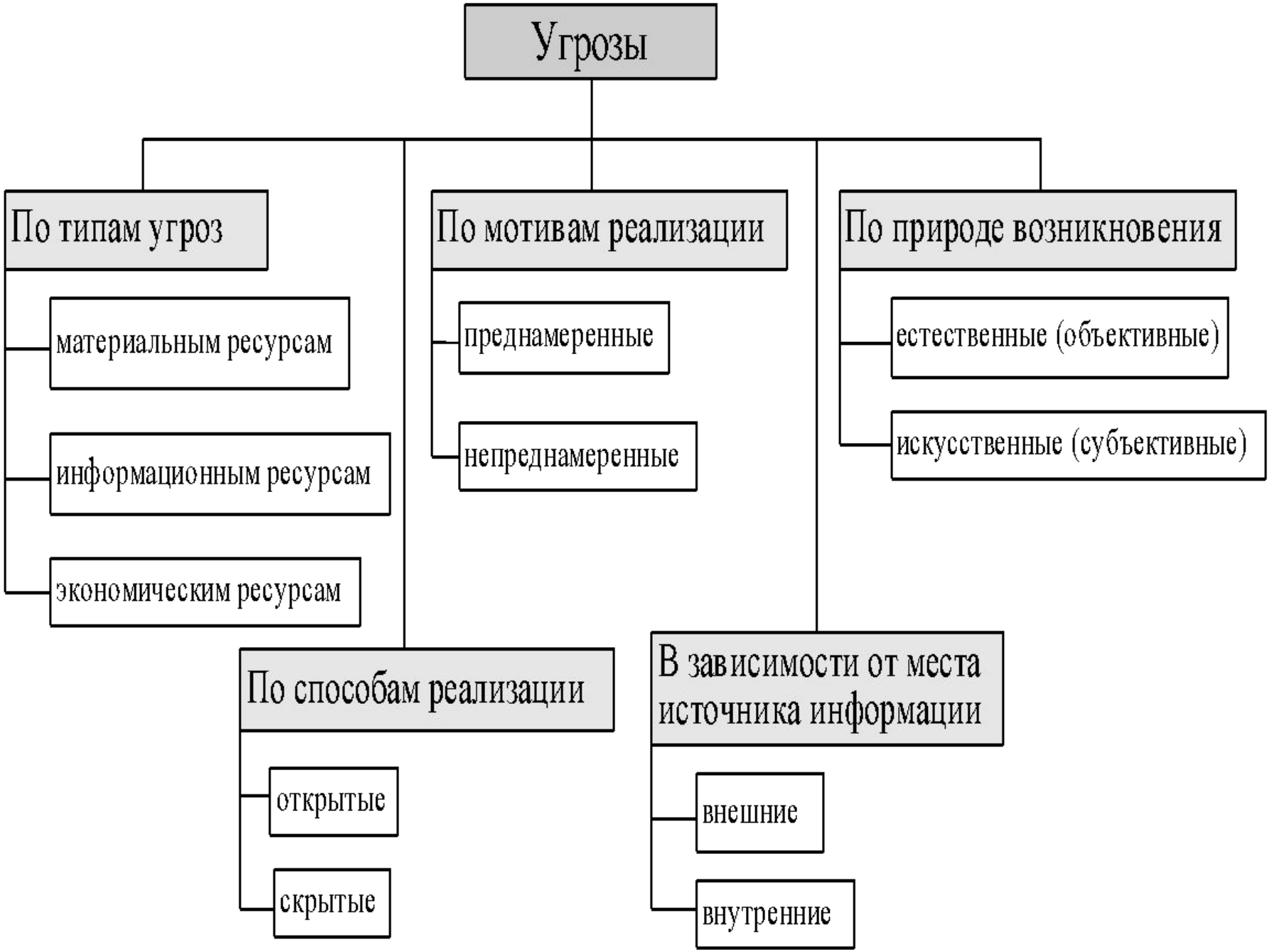
- Под угрозой понимают потенциальную возможность нарушения безопасности предприятия связи.
- Под моделью угроз будем понимают абстрактное (формализованное или неформализованное) описание совокупности потенциальных возможностей нарушения безопасности.

Модель угроз

- Возможные цели нарушителя
- Модель нарушителя
- Варианты возможных действий нарушителя
- Оценка риска

- **Модель угроз** содержит перечень возможных воздействий нарушителя на объекты охраны (целей и способов их достижения), а также модель нарушителя.
- Определение целей НСД, облика нарушителя и возможных вариантов его действий дает возможность сформировать систему охраны, позволяющую противостоять его действиям, обнаружить и локализовать нарушителя при попытке НСД на объекты предприятия.

- Рассмотрение возможных угроз проводится по следующим основным направлениям:
- безопасность персонала: неэффективная защита может привести к ущербу здоровью или даже угрозе жизни сотрудников;
- угрозы материальным ценностям, имуществу и оборудованию;
- безопасность информации.


Угрозы
По типам угроз
материальным ресурсам
информационным ресурсам
экономическим ресурсам
По мотивам реализации
преднамеренные
непреднамеренные
По природе возникновения
естественные (объективные)
искусственные (субъективные)
По способам реализации
открытые
скрытые
В зависимости от места источника информации
внешние
внутренние

Преднамеренные угрозы:

- захват заложников, физическое устранение руководящего состава и т.п. действия, ведущие к развалу объекта, системы в целом или другим последствиям;
- хищение материальных (финансовых) ресурсов, прежде всего денежных средств, средств связи, автоматизации, а также оборудования и других устройств, содержащих драгметаллы или представляющих другую ценность на рынке;
- порча, уничтожение материальных (финансовых) ресурсов и технологического и другого оборудования;
- организация деструктивного воздействия на технологический процесс с целью нанесения материального ущерба;
- хищение, уничтожение, ознакомление с носителями конфиденциальной информации, блокирование доступа к ним;
- получение доступа и/или нарушение работы средств автоматизированного управления технологическими процессами, средствами связи и информатизации и т. п.;
- подготовка к надежному вторжению путем саботажных действий над техническими средствами системы зашиты, нейтрализации группы охраны, ослабления инженерно-строительных средств защиты и т. п.;
- нанесение максимально возможного ущерба путем вандальных действий (пожар, взрыв, другие действия, ведущие к угрозе жизни персонала и т. п.) для создания беспорядков и паники, способствующих успешному проникновению на объект с одной из вышеперечисленных целей, или для совершения диверсионно-террористической акции.

- **Непреднамеренные угрозы**
- Перечень непреднамеренных угроз объектам содержит перечень возможных непреднамеренных или случайных воздействий персонала на объекты охраны, приводящих к нанесению им ущерба. К таким угрозам относятся ошибки или халатные действия персонала, приводящие:
- к выходу из строя отдельных элементов оборудования объекта и к снижению его производительности;
- к возникновению аварийных или чрезвычайных ситуаций на отдельных охраняемых объектах и в системе в целом;
- к возникновению аварийных или чрезвычайных ситуаций не только на самом объекте, но и за его пределами.

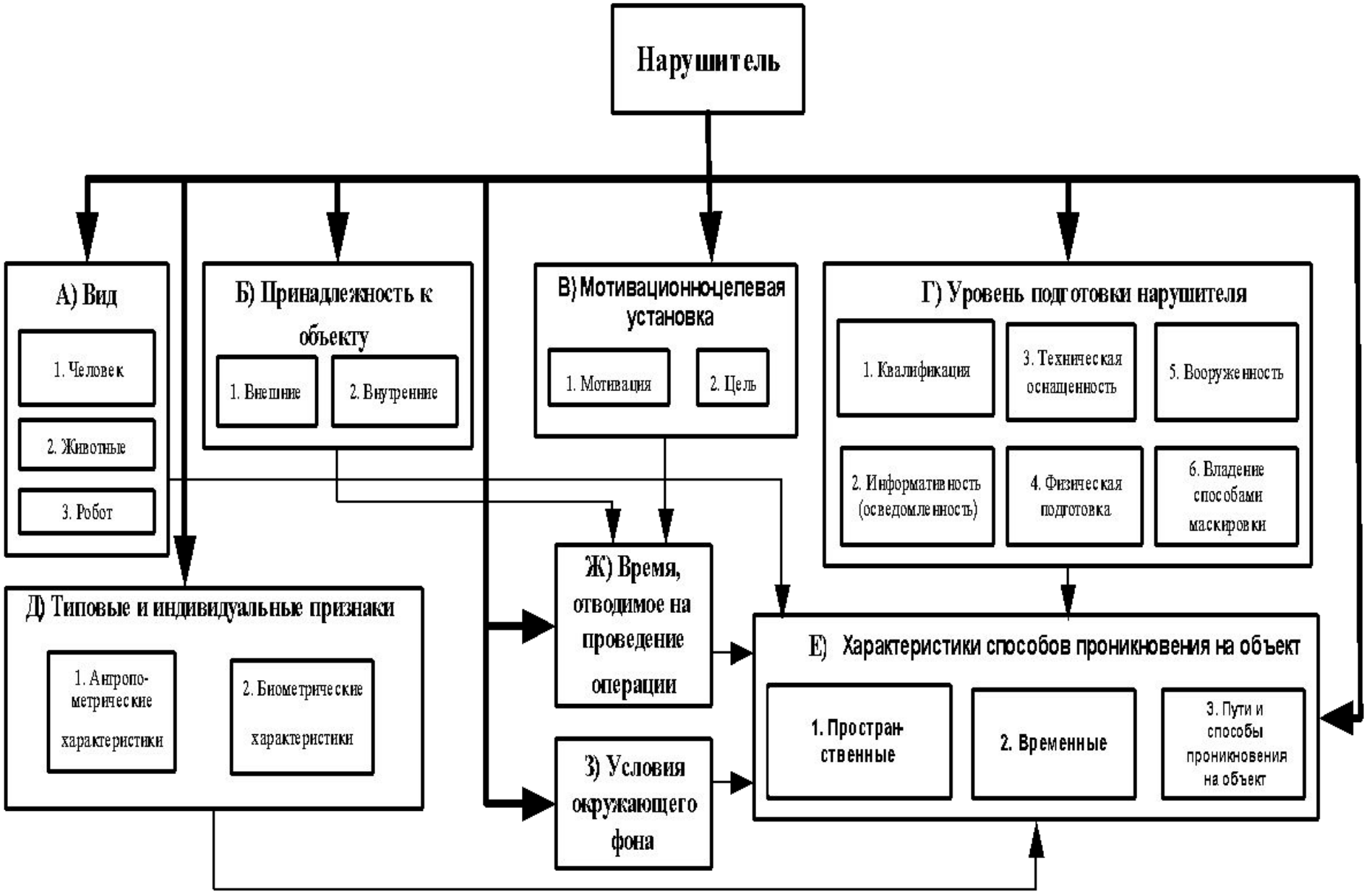
- **Техногенные угрозы**
- Перечень техногенных угроз объектам связи и информатизации содержит список возможных аварийных и чрезвычайных ситуаций техногенного характера, которые могут нанести им ущерб.
- Анализ показывает, что в перечень основных техногенных угроз объектам можно включить:
- пожар на охраняемом объекте;
- пожар на рядом расположенном объекте (угроза пожара, задымлений, разрушений в результате взрывов);
- повреждение (выход из строя) отдельно взятых элементов или участков (районов) технологических систем (независимо от причины их повреждения);
- разливы агрессивных жидкостей;
- опасные концентрации газов (вредных веществ);
- полные отключения электропитания.

- В зависимости от местонахождения источника информации все угрозы разделяют на две группы – внешние и внутренние.

- К *внешним угрозам* относятся:
- деятельность иностранных разведывательных и специальных служб;
- деятельность конкурирующих иностранных экономических структур;
- деятельность политических и экономических структур, преступных групп и формирований, а также отдельных лиц внутри страны, направленная против интересов граждан, государства и общества в целом и проявляющаяся в виде воздействий на ИТКС;
- стихийные бедствия и катастрофы.

- К *внутренним угрозам* относятся:
- нарушения установленных требований безопасности (непреднамеренные либо преднамеренные), допускаемые обслуживающим персоналом и пользователями;
- отказы и неисправности технических средств обработки, хранения и передачи сообщений (данных), средств защиты и средств контроля эффективности, принятых мер по защите;
- сбои программного обеспечения, программных средств защиты информации и средств контроля эффективности принятия мер по защите.

Модель нарушителя



Классификация нарушителей

- по квалификации: случайные, неподготовленные, подготовленные, обладающие специальной подготовкой (квалифицированные). Очевидно, что каждый тип нарушителей будет осуществлять проникновение на объект по-разному − менее грамотно или более грамотно (ухищренно), используя различные условия, способствующие проникновению.

- по информативности: неосведомленные, имеющие неполную информацию о системе охраны объекта; имеющие полную информацию о системе охраны объекта; имеющие неполную информацию об объекте (осведомлен о назначении объекта, его внешних признаках и чертах); имеющие полную информацию об объекте;

- по технической оснащенности (вооруженности): не оснащенные техническими приспособлениями (средствами), оснащенные стандартной техникой преодоления как инженерных, так и охранных систем; оснащенные специальной техникой, включающей в себя средства для преодоления инженерных и охранных систем, специальные технические средства негласного съема информации по техническим каналам утечки информации, специальные системы ночного, инфракрасного наблюдения, направленные микрофоны; не вооруженные, вооруженные, оснащенные специальными средствами для проведения террористических актов.

Возможные цели нарушителя

- хищение, порча, уничтожение материальных (финансовых) ресурсов, продукции, технологического и другого оборудования;
- организация деструктивного воздействия на технологический процесс с целью нанесения материального ущерба или подрыва репутации предприятия;
- хищение, модификация, уничтожение, ознакомление с конфиденциальной информацией, блокирование доступа к ней и получение доступа и/или нарушение работы средств информатизации и т.п.;
- организация хищения конфиденциальной информации путем создания искусственных либо использования естественных технических каналов ее утечки;
- подготовка к надежному вторжению путем саботажных действий на ТСО, нейтрализации группы охраны, ослабления инженерно-строительных средств защиты и т.п.;
- захват заложников, физическое устранение руководящего состава и т.п. действия, ведущие к развалу или подрыву репутации предприятия или другим последствиям;
- организация вандальных действий (пожар, взрыв, другие действия, ведущие к угрозе жизни персонала и т.п.) для создания беспорядков и паники, способствующих успешному проникновению на объект с одной из вышеперечисленных целей или как факт терроризма.