ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Техническими являются такие средства защиты, в которых основная защитная функция реализуется некоторым техническим устройством (комплексом, системой). **К достоинствам** технических средств относятся: широкий круг решаемых задач; высокая надежность; возможность создания развитых комплексных систем защиты; гибкое реагирование на попытки НСД; традиционность используемых методов осуществления защитных функций. **Основные недостатки**: высокая стоимость многих средств; необходимость регулярного проведения регламентных работ и контроля; возможность подачи ложных тревог.

Применение технических средств направлено на решение трех задач:

- предотвращение проникновения нарушителя к источникам информации;
- предотвращение повреждения носителя информации в результате воздействия стихийных сил и, прежде всего, пожаров, а также воды и пены при попадании;
- предотвращение утечки информации по различным техническим каналам.

Функции технических средств защиты:

- охрана территорий и зданий;
- охрана внутренних помещений;
- охрана оборудования и наблюдение за ним;
- контроль доступа в защищаемые зоны;
- нейтрализация излучений и наводок;
- создание препятствий визуальному наблюдению и прослушиванию;
- противопожарная защита;
- блокировка действий нарушителя.

Технические средства защиты информации подразделяются на две большие группы: инженерная защита и техническая охрана объектов (ИЗТОО) и сокрытие информации.

Инженерная защита и техническая охрана объектов (ИЗТОО) - метод защиты на основе инженерных конструкций в сочетании с техническими средствами охраны, в результате применения которого объекты защиты нейтрализованы в пространстве.

Сокрытие информации - предусматривает такие изменения структуры носителей, при которых нарушитель не может выделить информацию с качеством, достаточным для использования в собственных интересах, в результате чего объекты защиты не имеют четких границ.

Способы и средства инженерной защиты и технической охраны объектов (ИЗТОО).

Главной задачей ИЗТОО является недопущение непосредственного контакта нарушителя или сил природы с объектами защиты.

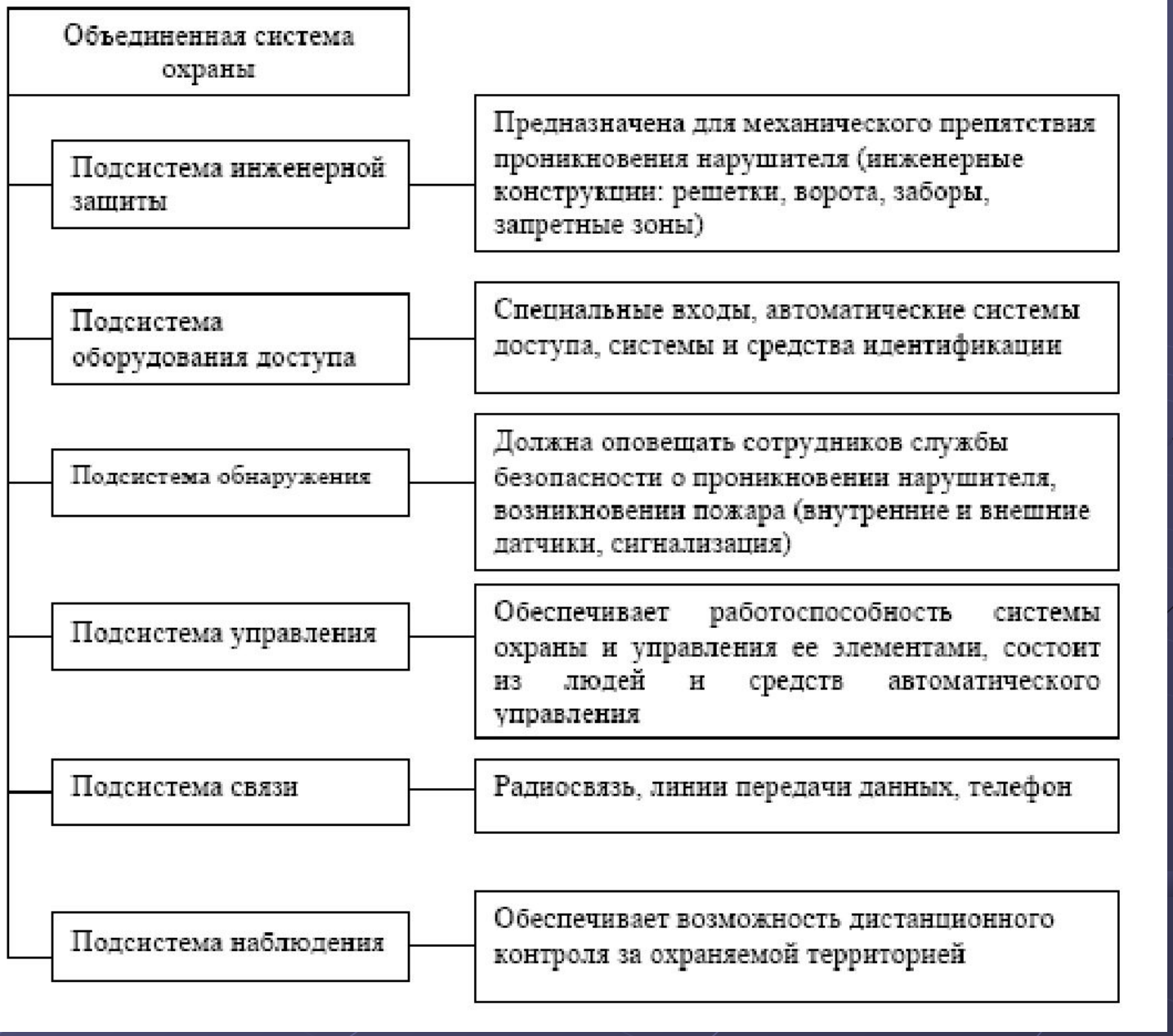
Основу ИЗТОО составляет:

1. Механические средства и инженерные сооружения, препятствующие физическому движению нарушителя к объектам защиты;
2. Технические средства, информирующие о проникновении нарушителя в контролируемую зону;

3. Технические средства наблюдения обстановки в контролируемой зоне;

4. Средства и люди, устраняющие угрозы.

Средства и люди ИЗТОО образуют систему обеспечения безопасности, в которую входят следующие подсистемы (Рисунок 1):


Объединенная система охраны
Подсистема инженерной защиты
Предназначена для механического препятствия проникновения нарушителя (инженерные конструкции: решетки, ворота, заборы, запретные зоны)
Подсистема оборудования доступа
Специальные входы, автоматические системы доступа, системы и средства идентификации
Подсистема обнаружения
Должна оповещать сотрудников службы безопасности о проникновении нарушителя, возникновении пожара (внутренние и внешние датчики, сигнализация)
Подсистема управления
Обеспечивает работоспособность системы охраны и управления ее элементами, состоит из людей и средств автоматического управления
Подсистема связи
Радиосвязь, линии передачи данных, телефон
Подсистема наблюдения
Обеспечивает возможность дистанционного контроля за охраняемой территорией

Подсистема инженерной защиты. Основой данной подсистемы являются механические или строительные элементы, создающие для нарушителя реальное физическое препятствие. Важнейшей характеристикой подсистемы инженерной защиты является *время сопротивления,* т.е. время, которое требуется злоумышленнику для ее преодоления. Исходя из требуемой величины названной характеристики, должен производиться и выбор типа инженерной защиты.

Подсистема оборудования доступа. При построении данной подсистемы рекомендуется:

- определить количество необходимых контрольно-пропускных пунктов, исходя из числа пропускаемых через них служащих, которых требуется проконтролировать с максимальной скоростью во время пиковой нагрузки;
- оценить требуемую степень безопасности организации, которую можно повысить, к примеру, путем дополнения устройств

считывания карточек средствами ввода персонального кода;

- предусмотреть средства аварийного выхода;
- оценить средства, необходимые на приобретение, установку и эксплуатацию данной подсистемы.

Подсистема обнаружения. Современные подсистемы обнаружения предполагают наличие тревожной сигнализации, в которой, в свою очередь, о попытках вторжения находят применение датчики нескольких типов. Поэтому основные характеристики подобных подсистем определяются, главным образом, характеристиками используемых датчиков.

Подсистема наблюдения. Наиболее широкое распространение в подобных подсистемах получили телевизионные установки дистанционного наблюдения. Вся контролируемая подсистемой наблюдения зона разграничивается на отдельные участки протяженностью не более 100 м, на которых устанавливается, по крайней мере, одна передающая телекамера. При разрабатывании датчиков подсистемы обнаружения изображение, передаваемое соответствующей телекамерой, автоматически выводится на экран монитора на центральном посту охраны.

Подсистема связи. Каналами связи могут быть специально проложенные проводные линии, телефонные линии объекта, телеграфные линии и радиосвязь. Наиболее распространенные каналы связи - многожильные экранированные кабели, которые для повышения надежности и безопасности работы помещают в металлические или пластмассовые трубы или металлорукава.

Подсистема нейтрализации угроз. Для предотвращения вторжения на охраняемую территорию используется оборонительная система, в которой находят применение осветительные и звуковые установки. Для задержания преступника предпринимают соответствующие оперативные меры.

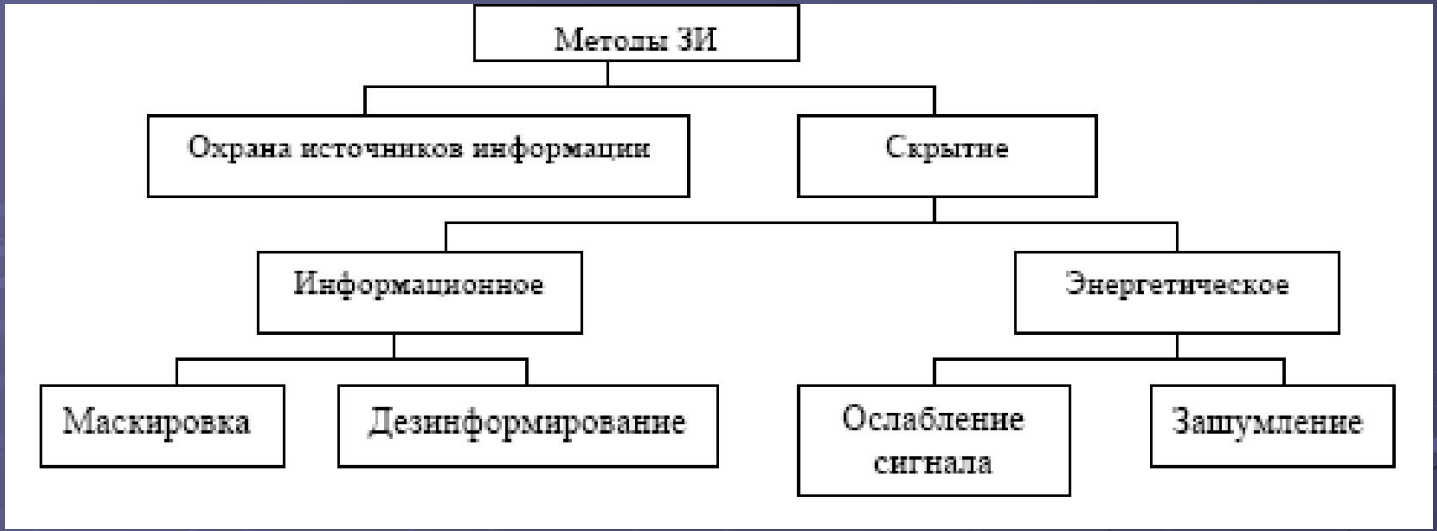
Подсистема управления. Сложные комплексы защиты охраняемых территорий, состоящие, как рассмотрено выше, из нескольких подсистем, могут эффективно функционировать только при условии, что работа всех технических установок постоянно контролируется и управляется с центрального поста. Он должен обеспечивать автоматическую регистрацию и отображение всех поступающих на центральный пост сообщений и сигналов тревоги, выполнение всех необходимых процедур.

Способы сокрытия защищаемой информации. Каждое устройство хранения, передачи и обработки информации является источником излучения различной природы (электромагнитные, акустические и другие волны). Перехватывая и обрабатывая излучения, сопровождающие работу информационных систем, возможно получать разнообразные сведения о процессах, сопровождающих передачу и обработку данных.

Данные электромагнитные излучения создают угрозы несанкционированного приема (перехвата) сигналов или, иначе говоря, технические каналы утечки информации.

Для защиты от подобного рода угроз применяют такое средство технической защиты, как **сокрытие информации**.

Сокрытие информации предусматривает такие изменения структуры, при которых нарушитель не может выделять информацию с качеством, достаточным для использования в своих интересах.



Сокрытие информации подразделяется на *информационное* и *энергетическое.*

Информационное сокрытие предусматривает изменение или создание ложного информационного портрета, семантического сообщения физического объекта или сигнала.

Информационный портрет – это совокупность элементов и связей между ними, отображающий смысл сообщения, признаки объекта или сигнала.

Возможны следующие способы изменения информационного портрета:

1. Удаление части элементов и связей, образующих информационный узел, т.е. наибольшую информационную часть портрета.
2. Изменение части элементов информационного портрета при сохранении неизменности связей между оставшимися элементами.

3. Удаление или изменение связей между элементами информационного портрета при сохранении их количества.

Средствами информационного сокрытия являются *маскировка* и *дезинформирование.*

Маскировка предусматривает изменение сигнала с целью затруднения его обнаружения среди других.

Дезинформирование заключается в трансформации исходного сигнала в новый, соответствующий ложной семантической информации и «навязывании» нового сигнала злоумышленнику.

Преимущества дезинформирования заключается в следующем: последствия решений принятых конкурентом на основе информации, могут быть для него худшими по сравнению с решениями, принимаемыми при отсутствии добытой информации.

Дезинформирование осуществляется путем подгонки признаков информационного портрета защищаемого объекта под признаки информационного портрета ложного объекта, соответствующего заранее разработанной версии.

Энергетическое сокрытие (ослабление сигнала, зашумление) предполагает уменьшение отношения энергии сигналов, т.е. носителей информации и помех.

Энергетическое сокрытие информации предусматривает использование таких средств как:

- электромагнитная экранировка помещений, в которых расположены элементы радиоэлектронной системы;
- применение в линиях и каналах связи волоконно-оптических кабелей, которые

обладают следующими преимуществами: отсутствие электромагнитного излучения во внешнюю среду, устойчивость к внешним электромагнитным излучениям, большая помехозащищенность, скрытность передачи, малые габариты, устойчивость к воздействиям агрессивной среды.

- активная радиотехническая маскировка подразумевает формирование и излучение в непосредственной близости от элементов радиоэлектронных систем маскирующего сигнала.