Тема 1.1. Цели и задачи физической защиты объектов информатизации

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Преподаватель: Сидиков И.Д.

Введение

Построение эффективной системы безопасности предприятия является актуальной задачей на сегодняшний день. Современное предприятие представляет собой большое количество разнородных компонентов, объединенных в сложную систему для выполнения поставленных целей, которые в процессе функционирования предприятия могут модифицироваться. Характерной особенностью подобных систем является, прежде всего, наличие человека в каждой из составляющих ее подсистем и отдаленность человека от объекта его деятельности. Это происходит в связи с тем, что множество компонентов, составляющих объект информатизации, интегрально может быть представлено совокупностью трех групп:

- люди (биосоциальные системы);
- техника (технические системы и помещения, в которых они расположены);
- программное обеспечение, которое является интеллектуальным посредником между человеком и техникой (интеллектуальные системы).

Введение

Все средства, методы и мероприятия, используемые для безопасности, наиболее рациональным образом объединяются в единый целостный механизм. Исходя из этого, решение проблемы обеспечения желаемого уровня защиты объекта информатизации невозможно без системного подхода, охватывающего выявление всех основных угроз, оценки возможного ущерба при реализации этих угроз и создания комплекса технических средств. Учет основных угроз жизни и здоровью, имуществу, ресурсам и информации позволяет выделить главные элементы комплексной системы безопасности:

- охранной сигнализации;
- охранно-пожарной сигнализации;
- телевизионного наблюдения;
- контроля и управления доступом;
- информационной безопасности и другие.

Введение

Очевидно, что это деление условно и реально такого четкого функционального разделения может не быть. Так системы охранной сигнализации, контроля доступа и системы ТВ наблюдения эффективно решают и задачи защиты информации, в частности доступа к информационным ресурсам и носителям информации.

Системный подход к построению системы безопасности включает в себя: прежде всего, изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца.

Системный подход — это принцип рассмотрения проекта, при котором анализируется система в целом, а не ее отдельные части. Его задачей является оптимизация всей системы в совокупности, а не улучшение эффективности отдельных частей. Это объясняется тем, что, как показывает практика, улучшение одних параметров часто приводит к ухудшению других, поэтому необходимо стараться обеспечить баланс противоречий требований и характеристик.

Основные понятия и определения

Функции и задачи физической защиты

Под физической защитой понимается совокупность организационных мероприятий, инженерно-технических средств, действий подразделений охраны в целях предотвращения диверсий или хищений носителей конфиденциальной информации и других материальных средств на охраняемых объектах.

Задачи физической защиты:

- предупреждение случаев несанкционированного доступа на объекты предприятия;
- своевременное обнаружение несанкционированных действий на территории предприятия;
- задержка (замедление) проникновения нарушителя, создание препятствий его действиям;
- пресечение несанкционированных действий на территории предприятия;
- задержание лиц, причастных к подготовке или совершению диверсии, хищению носителей конфиденциальной информации или иных материальных ценностей предприятия.

Основные понятия и определения

Физические средства защиты — разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников. К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа-выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Физические средства применяются для решения следующих задач:

1. Охрана территории и наблюдение за ней.
2. Охрана зданий, внутренних помещений и контроль за ними.
3. Охрана оборудования, продукции, финансов и информации.
4. Осуществление контроля доступа в здания и помещения.
5. Нейтрализация излучения и наводок.
6. Создание препятствий визуальному наблюдению.
7. Противопожарная защита.
8. Блокировка действий нарушителя.

Основные понятия и определения

Все физические средства защиты объектов можно разделить на три категории: средства предупреждения, средства обнаружения и системы ликвидации угроз. Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов — это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения и от других преступных действий. Средства пожаротушения относятся к системам ликвидации угроз.

Для предотвращения проникновения нарушителя на охраняемые объекты применяются следующие устройства: СВЧ, УЗ, ИК системы. Они предназначены для обнаружения движущихся объектов, определения их размеров, скорости и направления перемещения. Принцип их действия основан на изменении частоты отраженного от движущегося объекта сигнала (эффект Доплера). УЗ и ИК применяются в основном внутри помещений, а СВЧ - для охраны территорий и зданий. Лазерные и оптические системы работающие в видимой части спектра основаны на принципе пересечения нарушителем светового луча, применяются в основном в зданиях.

Основные определения

Допуск — разрешение на проведение определенной работы или на получение определенных документов и сведений.

Доступ — проход (проезд) в охраняемые зоны объекта предприятия;

Защищенная зона — территория объекта предприятия, которая окружена физическими барьерами, постоянно находящимися под охраной и наблюдением, и доступ в которую ограничивается и контролируется.

Нарушитель — лицо, совершившее или пытающееся совершить несанкционированное действие, а также лицо, оказывающее ему содействие в этом.

Несанкционированное действие — хищение или попытка хищения носителей конфиденциальной информации и материальных средств предприятия, осуществление или попытка осуществления несанкционированного доступа, проноса (провоза) запрещенных предметов, совершения диверсии, вывода из строя средств физической защиты.

Основные определения

Обнаружение — установление факта несанкционированного действия.

Функции обнаружения – оповещение о действиях нарушителя (тайных, открытых) с помощью датчиков или систем контроля доступа.

Датчики (извещатели) – средства обнаружения, бывают внешние или внутренние.

Задержка – замедление продвижения нарушителя.

Эффективность задержки – время, необходимое нарушителю после его обнаружения для преодоления каждого элемента задержки.

Элемент задержки – заграждения, замки, механические (активируемые) средства, отряд охраны.

Периметр — граница охраняемой зоны, оборудованная физическими барьерами и контрольно-пропускными пунктами.

Основные определения

Подразделение охраны — вооруженное подразделение, выполняющее задачи по охране и обороне объектов предприятия.

Система охранной сигнализации — совокупность средств обнаружения, тревожно-вызывной сигнализации, системы сбора, отображения и обработки информации.

Техническое средство обнаружения — устройство, предназначенное для автоматической подачи сигнала тревоги в случае несанкционированного действия.

Физический барьер — физическое препятствие, затрудняющее проникновение нарушителя в охраняемые зоны.

Ответные действия – предпринимаются охраной или специальными подразделениями для предотвращения успешного выполнения нарушителем своих задач.

Ответные действия – перехват и нейтрализация, важность связи между силами охраны.

Контроль и управления доступом

Комплекс мероприятий, направленных на ограничение и санкционирование перемещение людей, предметов, транспорта в помещениях, зданиях, сооружениях и по территории объектов. Совокупность организационных мер, оборудования и приборов, инженерно-технических сооружений, алгоритмов и программ, которая автоматически выполняет в определенных точках объекта в заданные моменты времени следующие основные задачи: разрешает проход уполномоченным субъектам (сотрудникам, посетителям, транспорту); запрещает проход всем остальным.

В целях физической защиты территории и объектов предприятия решением его руководителя создается система физической защиты (СФЗ), предназначенная для удержания нарушителей от совершения противоправных действий или их обнаружения и задержки, принятия ответных мер. Эта система создается исходя из необходимости и целесообразности при условии невозможности эффективного решения ранее перечисленных задач с использованием традиционных сил и средств охраны предприятия.

Система физической защиты

Система физической защиты (СФЗ) предприятия включает:

1. Организационные мероприятия;
2. Инженерно-технические средства;
3. Действия подразделений охраны.

К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Термины, относящиеся к угрозам безопасности информации

– угроза (безопасности информации): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

– фактор, воздействующий на защищаемую информацию: явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней;

– источник угрозы безопасности информации: субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации;

– уязвимость (информационной системы); брешь: свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе. Если уязвимость соответствует угрозе, то существует риск.

Термины, относящиеся к угрозам безопасности информации

Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе. Если уязвимость соответствует угрозе, то существует риск.

Преднамеренное силовое электромагнитное воздействие на информацию: несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования технических и программных средств этих систем.

Модель угроз (безопасности информации): физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Основные виды источников и носителей защищаемой информации

С точки зрения защиты информации ее источниками являются субъекты и объекты, от которых информация может поступить к несанкционированному получателю (злоумышленнику). Очевидно, что ценность этой информации определяется информированностью источника. Основными источниками информации являются следующие:

1. люди;
2. документы;
3. продукция;
4. измерительные датчики;
5. интеллектуальные средства обработки информации;
6. черновики и отходы производства;
7. материалы и технологическое оборудование.

Основные виды источников и носителей защищаемой информации

Основные объекты защищаемой информации можно объединить в следующие группы:

- собственники, владельцы и пользователи;
- носители и технические средства передачи и обработки информации;
- системы информатизации связи и управления, военная техника;
- объекты органов управления, военные и промышленные объекты.

В целях обеспечения безопасности, прежде всего, необходимо обеспечить защиту прав собственников и пользователей информацией в сфере информационных процессов и информации, а так же определить их обязанности и ответственность за нарушение режима защиты информационных ресурсов.

Основные виды источников и носителей защищаемой информации

В группе носителей и технических средств передачи и обработки информации защите подлежат следующие объекты:

1. носители информации в виде информационных физических полей, химических сред, сигналов, документов на различных основах;
2. средства вычислительной техники;
3. средства связи;
4. средства преобразования речевой информации;
5. средства визуального отображения;
6. средства размножения документов;
7. вспомогательные технические средства, расположенные в помещении, где информация обрабатывается;
8. помещения, выделенные для проведения мероприятий.

Основные виды источников и носителей защищаемой информации

В интересах ЗИ о вооружении и военной технике защите подлежат:

1. характеристики и параметры конкретных образцов вооружений и военной техники на всех этапах их жизненного цикла;
2. научно-исследовательские, опытно-конструкторские и экспертные работы военно-прикладной направленности.

Для объектов органов управления, военных промышленных объектов защите подлежит следующая информация:

1. о местоположении объекта;
2. о предназначении, структуре объекта и режимах его функционирования;
3. информация, циркулирующая в технических средствах, используемых на объекте;
4. информация о разрабатываемых и эксплуатационных образцах вооружения, военной техники и технологии;
5. информация о научно-исследовательских и опытно-конструкторских работах.

Разработка граф-структуры защищаемой информации

Для структурирования информации в качестве исходных данных используется перечень сведений составляющих государственную, ведомственную или коммерческую тайну, а также перечень источников информации в организации. Структурирование информации производится путем классификации информации в соответствии с функциями, задачами и структурой организации с привязкой элементов информации к ее источникам.

Схема классификации разрабатывается в виде графа-структуры, причем нулевой (верхний) уровень иерархической структуры соответствует понятию «защищаемая информация». Нижний уровень соответствует элементам информации одного источника из перечня источников информации.

Разработка граф-структуры защищаемой информации

Результаты структурирования оформляются в виде таблиц.
Структурная модель объекта защиты – вербальная модель, таблица со столбцами:

– номер элемента информации,

– наименование элемента информации,

– гриф конфиденциальности,

– цена информации,

– наименование источников информации,

– местонахождение источников информации.

Моделирование объекта защиты

Моделирование объекта защиты включает в себя:

1. определение источников защищаемой информации,
2. описание пространственного расположения основных мест размещения источников защищаемой информации,
3. выявление путей распространения носителей защищаемой информации за пределы контролируемых зон,
4. описание объекта защиты с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

Моделирование объекта защиты

Моделирование проводится на основе пространственных моделей контролируемых зон с указанием мест расположения источников защищаемой информации. Это планы помещений, этажей, зданий, территории в целом.

Моделирование состоит в анализе на основе рассмотренных пространственных моделей того, какие могут быть пути распространения информации за пределы контролируемой зоны, и в определении уровней полей и сигналов на границах контролируемых зон. Уровни полей и сигналов рассчитываются с учетом уменьшения мощности на выходе источников сигнала (в дБ) на суммарную величины их ослабления в среде распространения. В результате моделирования объекта защиты оценивается состояние безопасности информации и определяются слабые места существующей системы защиты. Результаты моделирования отображаются в виде таблиц.

Определение категории важности информации

Основным признаком конфиденциальной информации является ее ценность для потенциального противника (конкурентов). Поэтому, определяя перечень сведений конфиденциального характера, их обладатель должен определить эту ценность через меру ущерба, который может быть нанесен предприятию при их утечке (разглашении). В зависимости от величины ущерба (или негативных последствий), который может быть нанесен при утечке (разглашении) информации, вводятся следующие категории важности информации:

- 1 категория – информация, утечка которой может привести к потере экономической или финансовой самостоятельности предприятия или потери ее репутации (потери доверия потребителей, смежников, поставщиков и т.п.);
- 2 категория – информация, утечка которой может привести к существенному экономическому ущербу или снижению ее репутации;
- 3 категория – информация, утечка разглашение которой может нанести экономический ущерб предприятию.

Определение категории важности информации

С точки зрения распространения информации на две группы:

- первая группа (1) – конфиденциальная информация, которая циркулирует только на предприятии и не предназначенная для передачи другой стороне;

- вторая группа (2) – конфиденциальная информация, которая предполагается к передаче другой стороне или получаемая от другой стороны.

Следовательно, целесообразно установить шесть уровней конфиденциальности информации (таблица 1).

Введение категорий конфиденциальности информации необходимо для определения объема и содержания комплекса мер по ее защите.

При установлении режима доступа к конфиденциальной информации необходимо руководствоваться принципом - чем больше ущерб от разглашения информации, тем меньше круг лиц, которые к ней допущены.

Определение категории важности информации

Величина ущерба (негативных последствий), который может быть нанесен при разглашении конкретной информации	Уровень конфиденциальности информации	
	информация, не подлежащая передаче другим предприятиям (организациям)	информация, предназначенная для передачи другим предприятиям (организациям) или полученная от них
Утечка информации может привести к потере финансовой самостоятельности предприятия или потери ее репутации	1.1	1.2
Утечка информации может привести к существенному экономическому ущербу или снижению репутации предприятия	2.1	2.2
Утечка информации может нанести экономический ущерб предприятию	3.1	3.2

Основные задачи физической защиты

1) Предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения материальных ценностей.

2) Защита объекта от воздействия стихийных сил: пожара и воды.

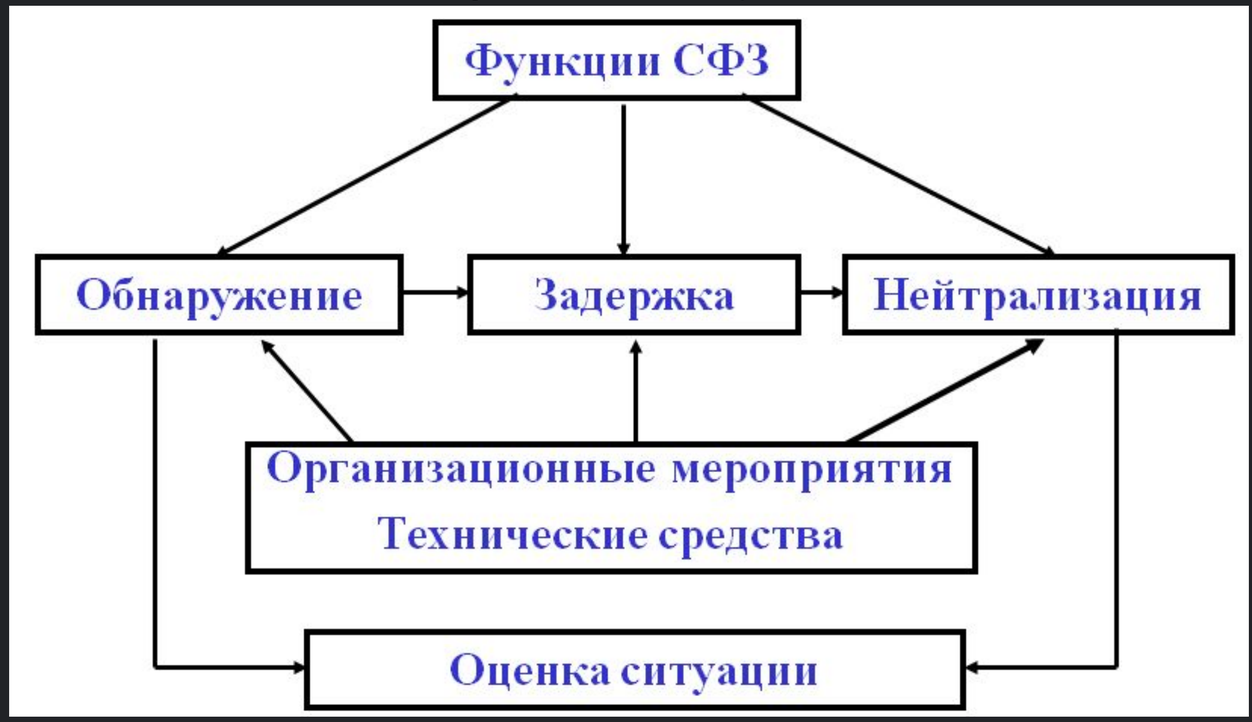
Решение задач направлено на сведения к минимуму:

- возможностей несанкционированного проникновения на объект;
- сведения к минимуму вероятности осуществления актов промышленного шпионажа;
- последствий от воздействия стихии.

Основные задачи системы физической защиты представлены на рисунке 2.

Основные задачи физической защиты

Обнаружение – раскрытие действий, совершаемых нарушителями. Функции обнаружения – оповещение о действиях нарушителя (тайных, открытых) с помощью датчиков или систем контроля доступа. Датчики (извещатели) – внешние или внутренние. Ответные действия – предпринимаются охраной или спец.подразделениями для предотвращения успешного выполнения нарушителем своих задач. Ответные действия – перехват и нейтрализация. Ответные действия – важность связи между силами охраны.



Формулирование принципов построения системы физической защиты

Принципы (общие):

- Непрерывность (постоянная готовность к отражению угроз);
- «Угроза» - потенциальная возможность совершения действий, направленных на нарушение безопасности объекта
- Активность (прогнозирование, реализация опережающие действия);
- Скрытность (средств и процедур защиты);
- Целеустремленность (предотвращение угроз наиболее ценным составляющим объекта);
- Комплексность (использование различных способов и средств защиты).

Формулирование принципов построения системы физической защиты

Принципы (специальные):

- соответствие уровня защиты ценности информации;
- гибкость защиты;
- Многозональность (разбиение объекта на защищаемые (контролируемые) зоны; дифференцированный санкционированный доступ в защищаемую зону);
- Многорубежность (разбиение объекта на рубежи защиты – границы зон);
- Равнопрочность (сбалансированность).

Первый принцип определяет экономическую целесообразность применения тех или иных средств мер защиты. Он заключается в том, что затраты на защиту информации не должны превышать цену защищаемой информации.

Так как цена информации - величина переменная, зависящая как от источника информации, так и от времени, то во избежание неоправданных расходов защита информации должны быть гибкой. Гибкость защиты проявляется в возможности изменения степени защищённости в соответствии с изменившимися требованиями к информационной безопасности.

Формулирование принципов построения системы физической защиты

Требуемый уровень информационной безопасности достигается многозональностью и многорубежностью защиты. Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к источникам информации и реализуется путём разделения пространства, занимаемого объектом защиты на так называемые контролируемые зоны.

Типовыми зонами являются:

- территория занимаемая объектом защиты и ограниченная забором или условной внешней границей;
- здание на территории;
- коридор или его часть;
- помещение;
- шкаф, сейф, хранилище.

Формулирование принципов построения системы физической защиты

Зоны могут быть независимыми (здания, помещения), пересекающимися и вложенными (сейф в комнате, комната в здании, здание на территории). С целью воспрепятствования проникновению злоумышленника в зону на её границе создаются, как правило, один или несколько рубежей защиты. Рубежи защиты создаются и внутри зоны на пути возможного движения злоумышленника или распространения иных носителей, прежде всего, электромагнитных и акустических полей. Каждая зона характеризуется уровнем безопасности находящейся в ней информации. Информационная безопасность зависит от:

- расстояния от источника информации (сигнала) до злоумышленника или его средств добывания информации;
- количества и уровня защиты рубежей на пути движения злоумышленника или распространения иного носителя информации;
- эффективности способов и средств управления допуском людей и автотранспорта в зону;
- мер по защите информации внутри зоны.

Формулирование принципов построения системы физической защиты

Чем больше удалённость источника информации от места нахождения злоумышленника или его средства добывания информации и чем больше рубежей защиты, тем больше время движения злоумышленника к источнику и ослабление энергии носителя в виде поля или электрического тока. Количество и пространственное расположение зон и рубежей выбирается таким образом, чтобы обеспечить требуемый уровень информационной безопасности как от внешних (вне территории организации), так и внутренних (проникших на территорию злоумышленников или сотрудников) факторов атаки на защищаемый объект. Чем более ценной является информация, тем большим количеством рубежей и зон целесообразно окружить её источник.

Формулирование принципов построения системы физической защиты

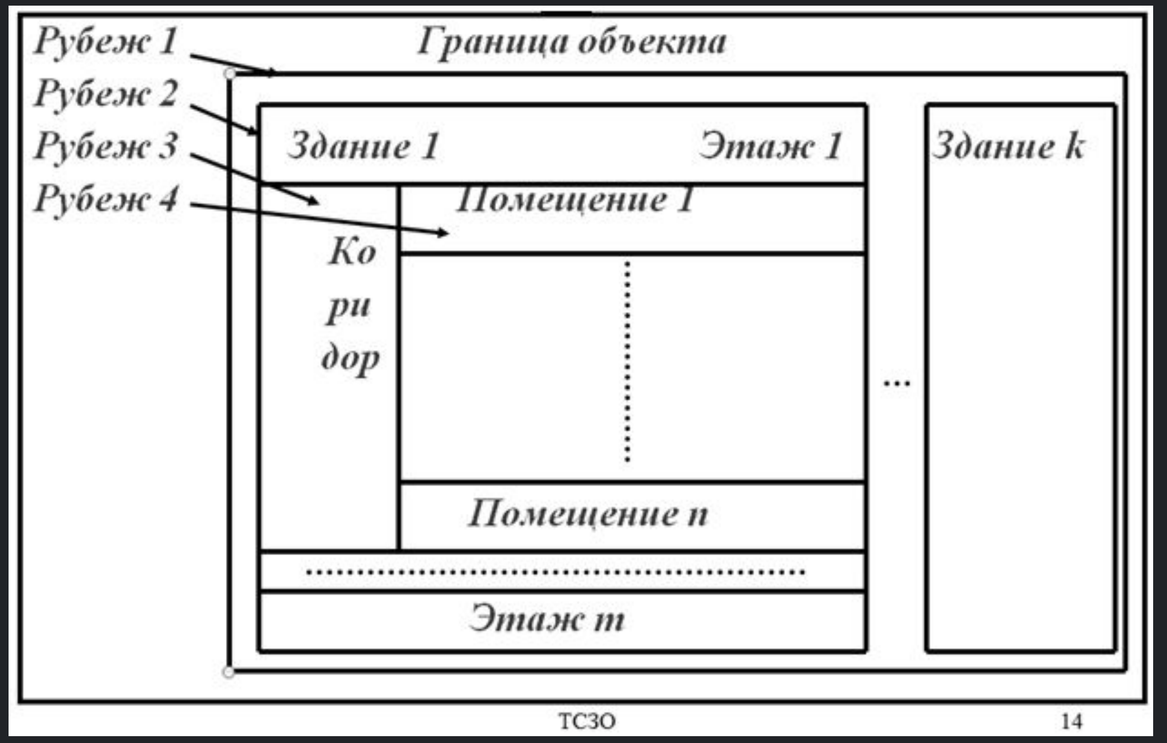
Рассмотренные выше принципы относятся к защите информации в целом. При построении системы защиты информации нужно учитывать также следующие принципы:

- минимизация дополнительных задач и требований к сотрудникам организации, вызванных мерами по защите информации
- надёжность в работетехнических средств системы, исключающая как нереагирование на угрозы (пропуски угроз) информационной безопасности, так и ложные реакции при их отсутствии;
- ограниченный и контролируемый доступ к элементам системы обеспечения информационной безопасности;
- непрерывность работы системы в любых условиях функционирования объекта защиты, в том числе, например, кратковременном отключении электроэнергии;
- адаптируемость системы к изменениям окружающей среды.

Формулирование принципов построения системы физической защиты

Наилучшая система защиты (абсолютная система защиты) – обладает всеми возможными способами (метод+средство) защиты, способна в любой момент своего существования прогнозировать наступление угрожающих событий во времени, достаточном для приведения в действие адекватных мер.

Пример построения многорубежной защиты приведен на рисунке 3.



Построение модели вероятного нарушителя

Под моделью нарушителя понимается совокупность количественных и качественных характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны и/или его составным частям.

Составляющие модели нарушителя:

- категории нарушителя и его возможные тактические методы (внешние, внутренние, внешние в сговоре с внутренними);
- возможные действия нарушителя (применение силы, хищение, дезинформация и т.д.);
- причины и мотивы действий нарушителя (корысть, принуждение и т.д);
- возможности нарушителя (навык, опыт, количество, оснащенность-техника, оружие, транспорт).

«Внешний нарушитель» - нарушитель из числа лиц, не имеющих права доступа в охраняемые зоны;
«Внутренний нарушитель» - нарушитель из числа лиц, имеющих право доступа без сопровождения в охраняемые зоны;
«Внешняя угроза» - угроза, исходящая от внешнего нарушителя;
«Внутренняя угроза» - угроза, исходящая от внутреннего нарушителя.

Построение модели вероятного нарушителя

Для описания моделей нарушителей в качестве критериев классификации рассматриваются:

1. Цели и задачи вероятного нарушителя:

- проникновение на охраняемый объект без причинения объекту видимого ущерба;
- причинение ущерба объекту;
- преднамеренное проникновение при отсутствии враждебных намерений;
- случайное проникновение.

2. Степень принадлежности вероятного нарушителя к объекту:

- вероятный нарушитель - сотрудник охраны;
- вероятный нарушитель - сотрудник учреждения;
- вероятный нарушитель - посетитель;
- вероятный нарушитель - постороннее лицо.

Построение модели вероятного нарушителя

3. Степень осведомленности вероятного нарушителя об объекте:

- детальное знание объекта;
- осведомленность о назначении объекта, его внешних признаках и чертах;
- неосведомленный вероятный нарушитель.

4. Степень осведомленности нарушителя о системе охраны объекта:

- полная информация о системе охраны объекта;
- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;
- информация о системе охраны вообще, но не о системе охраны конкретного объекта;
- неосведомленный вероятный нарушитель.

Построение модели вероятного нарушителя

5. Степень профессиональной подготовленности вероятного нарушителя:

- специальная подготовка по преодолению систем охраны;
- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

6. Степень физической подготовленности вероятного нарушителя:

- специальная физическая подготовка;
- низкая физическая подготовка.

7. Владение вероятным нарушителем способами маскировки.

8. Степень технической оснащенности вероятного нарушителя.

9. Способ проникновения вероятного нарушителя на объект.

Построение модели вероятного нарушителя

На основе изложенных критериев выделяют четыре категории нарушителя:

1. нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;

2. нарушитель второй категории - непрофессиональный нарушитель с враждебными намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект;

3. нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;

4. нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

Построение модели вероятного нарушителя

Модели нарушителя по типу бывают: неформализованные,
формализованные.

Неформализованная модель нарушителя представляет собой словесное описание его, отражает причины и мотивы действий, его возможности, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей, способы реализации исходящих от него угроз, место и характер действия, возможная тактика.

Формализованная модель нарушителя представляет собой математическое описание его, которое обычно строится на основе теории игр, когда для создания защитной системы используется матрица угроз/средств защит и матрица вероятностей наступления угроз. Типовая модель нарушителя представлена на рисунке 4.

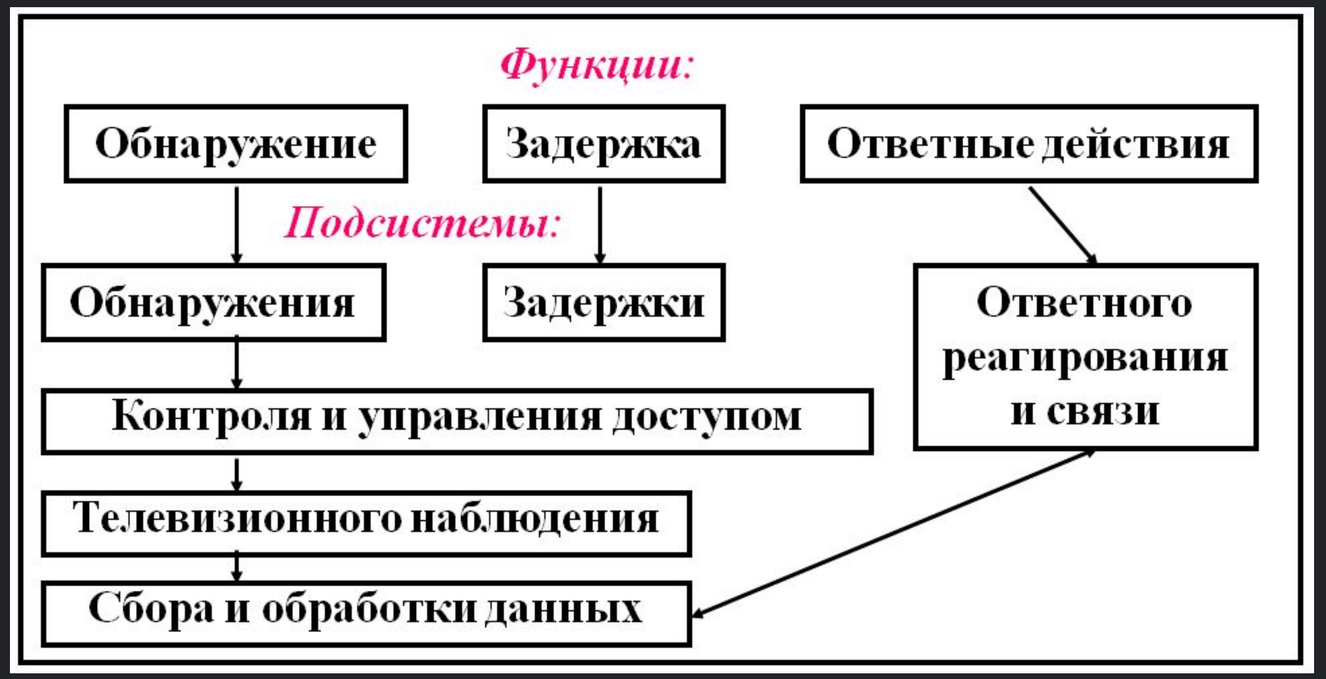
Построение модели вероятного нарушителя

Тип	Категория	Подготовленность								
		Психофизическая			Техническая			Осведомленность		
		Выс	Ср	Низк	Выс	Ср	Низк	Выс	Ср	Низк
Внешний	Специалист	+			+			+		
	Любитель		+			+			+	
	Дилетант			+			+			+
Внутренний	Сотрудник		+			+		+		

Функциональная структура СФЗ объекта

Функциональная структура системы физической защиты включает:

- службу безопасности (управление и координация всей деятельности по физической защите);
- силы охраны (охрана зон);
- комплекс физических барьеров и инженерных сооружений;
- комплекс технических и программных средств и систем (обнаружение, наблюдение, управление доступом, сбор, обработка и отображение информации, связь).



Разработка плана организационно-технических мероприятий

Инженерно-техническая защита информации на объекте достигается выполнением комплекса организационно-технических и технических мероприятий с применением средств защиты информации от утечки информации или несанкционированного воздействия на нее по техническим каналам.

Организационно-технические мероприятия основаны на введении ограничений на условия функционирования объекта защиты и являются первым этапом работ по защите информации. Эти мероприятия нацелены на оперативное решение вопросов защиты наиболее простыми средствами и организационными мерами ограничительного характера, регламентирующими порядок пользования техническими средствами. Они, как правило, проводятся силами и средствами служб безопасности самих предприятий и организаций.

Разработка плана организационно-технических мероприятий

В процессе организационных мероприятий необходимо определить:

а) контролируемую зону (зоны).

Контролируемая зона может ограничиваться:

- периметром охраняемой территории предприятия;
- частью охраняемой территории, охватывающей здания и сооружения, в которых проводятся закрытые мероприятия;
- частью здания (комнаты, кабинеты, залы заседаний, переговорные помещения, в которых проводятся закрытые мероприятия).

Бывают постоянная и временная контролируемые зоны. Постоянная контролируемая зона - зона, граница которой устанавливается на длительный срок. Постоянная зона устанавливается в случае, если конфиденциальные мероприятия внутри этой зоны проводятся регулярно. Временная контролируемая зона - зона, установленная для проведения конфиденциальных мероприятий разового характера.

Разработка плана организационно-технических мероприятий

б) выделить из эксплуатируемых технических средств технические средства, используемые для передачи, обработки и хранения конфиденциальной информации (ОТСС).

ОТСС - технические средства, предназначенные для передачи, обработки и хранения конфиденциальной информации. К ним относятся:

- системы внутренней (внутриобъектовой) телефонной связи;
- директорская, громкоговорящая диспетчерская связь;
- внутренняя служебная и технологическая системы связи;
- переговорные устройства типа «директор-секретарь»;
- системы звукоусиления конференц-залов, залов совещаний, столов заседаний, звукового сопровождения закрытых кинофильмов;
- системы звукозаписи и звуковоспроизведения (магнитофоны, диктофоны).

Разработка плана организационно-технических мероприятий

в) выявить в контролируемой зоне (зонах) вспомогательные технические средства и системы (ВТСС).

ВТСС - средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной (секретной) информации, на которые могут воздействовать электрические, магнитные и акустические поля опасных сигналов. К ним могут относиться:

- системы звукоусиления, предназначенные для обслуживания несекретных мероприятий;
- различного рода телефонные системы, предназначенные для несекретных переговоров и сообщений (городская телефонная связь, системы внутренней телефонной связи с выходом и без выхода в город);
- несекретная директорская, громкоговорящая диспетчерская, внутренняя служебная и технологическая связь, переговорные устройства типа «директор-секретарь»;
- системы специальной охранной сигнализации (ТСО), технические средства наблюдения;

Разработка плана организационно-технических мероприятий

- системы пожарной сигнализации;
- системы звуковой сигнализации;
- системы кондиционирования;
- системы проводной, радиотрансляционной сети радиовещания;
- телевизионные абонентские системы;
- системы электрочасофикации (первичная, вторичная);
- системы звукозаписи и звуковоспроизведения несекретной речевой информации (диктофоны, магнитофоны);
- системы электроосвещения и бытового электрооборудования (светильники, настольные вентиляторы, проводная сеть электроосвещения);
- электронная оргтехника - множительная, вычислительная техника.

Разработка плана организационно-технических мероприятий

- г) уточнить назначение и необходимость применения ВТСС в производственных и управленческих циклах работы;

- д) выявить технические средства, применение которых не обосновано служебной необходимостью;

- е) выявить наличие задействованных и незадействованных воздушных, наземных, подземных, настенных, а также заложенных в скрытую канализацию кабелей, цепей, проводов, уходящих за пределы контролируемой зоны;

- ж) составить перечень выделенных помещений первой и второй групп, в которых проводятся или должны проводиться закрытые мероприятия (переговоры, обсуждения, беседы, совещания) и помещений третьей группы.