Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра вычислительной техники

Е.В. Бурькова

ФИЗИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Рекомендовано к изданию Редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет» в качестве методических указаний для студентов, обучающихся по программе высшего профессионального образования по направлению подготовки 090900.62 Информационная безопасность

Оренбург
2012

УДК 004.56.53(076.5)
ББК 32.973-04 я7
Б 91

Рецензент – кандидат технических наук, доцент А.В. Хлуденев

Бурькова Е.В.

Б 91 Физические средства защиты объектов информатизации: методические указания к лабораторным работам / Е.В. Бурькова; – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2012. – 54 с.

В методических указаниях представлены теоретические сведения об этапах моделирования системы физической безопасности объектов. Методические указания содержат материалы для проведения лабораторных работ по курсу «Физические средства защиты объектов информатизации», приведены примеры моделей, даны задания, вопросы для самопроверки.

Методические указания предназначены для студентов направления подготовки 090900.62 Информационная безопасность.

УДК 004.56.53(076.5)
ББК 32.973-04 я7

Содержание

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).

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.

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.

Данные методические указания предназначены для проведения лабораторных работ по курсу «Физические средства защиты объектов информатизации» для студентов направления подготовки 090900.62 «Информационная безопасность».

Методические указания содержат пять разделов, в которых даны теоретические сведения об этапах моделирования систем физической безопасности объектов информатизации, примеры моделей, даны задания, вопросы для самопроверки.

1 Основные понятия и определения

1.1 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.

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.

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.

1.2 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.

Несанкционированный доступ — проникновение лиц, не имеющих права доступа, в охраняемые зоны, на объекты, в служебные помещения предприятия.

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.

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 управление 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 (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.

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.

1.3 Варианты объектов физической защиты

В таблице 1.1 представлены варианты объектов информатизации, для которых необходимо провести анализ защищаемой информации, угроз, разработать модель системы физической защиты, рассчитать эффективность предложенных мер в соответствии с заданиями лабораторных работ.

Таблица 1.1 - Варианты объектов защиты

№ варианта	Объект информатизации
1	Бухгалтерия завода железобетонных изделий
2	Помещения дирекции торгового центра
3	Медпункт учебного корпуса университета
4	Деканат факультета университета
5	Отдел главного конструктора приборного завода
6	Зал переговоров фирмы по изготовлению лекарственных средств
7	Следственный отдел прокуратуры
8	Помещение группы программистов коммерческого банка
9	Патентный отдел завода
10	Редакция научного издания
11	Отдел научно-исследовательского института
12	Помещения диссертационного совета университета
13	Рекламное агентство
14	Отдел кадров завода бурового оборудования
15	Конструкторское бюро завода оборонной промышленности

2 Лабораторная работа № 1. Моделирование объекта защиты

Цель. Анализ характеристик защищаемого объекта, определение задач и функций СФЗ.

Задачи.

1) Описание объекта защиты, характеристика назначения объекта.
2) Построение структурной модели конфиденциальной информации.
3) Разработка граф-структуры защищаемой информации.
4) Определение категории защищаемой информации.
5) Определение задач и функций СФЗ.
6) Формулирование принципов построения СФЗ.

2.1 Описание объекта защиты

Задание 1.

1) Параметры объекта. В соответствии с вариантом задания определить границы территории объекта, описать расположение здания, планировку здания и определить все точки доступа на территорию объекта. Разработать план помещений объекта, описать расположение оборудования, заполнить таблицу 2.1.

Таблица 2.1 – Описание объекта защиты

№	Наименование параметра	Данные
1	Площадь, кв.м.	
2	Высота потолка.	
3	Толщина стен: наружных, внутренних.	
4	Окна: количество, размер.	
5	Двери: размер проема, тип, замок.	
6	Описание смежных помещений: сверху, сбоку слева, сбоку справа, снизу.	
7	Система электропитания (освещение): тип светильников и их количество.	
8	Система заземления.	
9	Системы сигнализации.	
10	Система вентиляции (тип).	
11	Наличие экранов на батареях.	
12	Телефонные линии: городская сеть, тип розеток.	

2) Описание рабочих процессов на объекте. Привести описание ведущихся на объекте работ, дать характеристику операций, выполняемых на объекте и условий их выполнения. Сформулировать назначение объекта.

3) Описание обстановки вокруг объекта. Провести анализ месторасположения объекта (в какой части города расположен объект), какие объекты находятся в ближайшем окружении. Составить пространственную модель объекта по примеру таблицы 2.2.

Таблица 2.2 - Пространственная модель контролируемых зон

№ п.п	**Пространственная характеристика помещения**	**Функциональная, конструктивная и техническая характеристика помещения**		
1	Этаж	2	Площадь, $м^2$	56
2	Количество окон, тип сигнализации, наличие штор на окнах	3 окна, жалюзи на окнах, плотные шторы, датчики разбития стекла «Breakglass 2000», F2, Y2, M1:2	Куда выходят окна	Проспект Сталинграда
3	Двери, кол-во, одинарные, двойные	4 двери звукоизолирующие тяжелые	Куда выходят двери	Коридор, каб. №3, каб. №2, каб. №1
4	Соседние помещения, название, толщина стен	1.С западной стороны находится Помещение №3. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича) 2. С восточной стороны расположен коридор. отштукатуренная с двух сторон стена (толщина - 1,5 кирпича)		

2.2 Построение структурной модели конфиденциальной информации

Для создания полной модели объекта защиты необходимо проанализировать защищаемую информацию и провести её структурирование.

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:

- люди;
- документы;
- продукция;
- измерительные датчики;
- интеллектуальные средства обработки информации;
- черновики и отходы производства;
- материалы и технологическое оборудование.

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.

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

- носители информации в виде информационных физических полей, химических сред, сигналов, документов на различных основах;
- средства вычислительной техники;
- средства связи;
- средства преобразования речевой информации;
- средства визуального отображения;
- средства размножения документов;

– вспомогательные технические средства, расположенные в помещении, где информация обрабатывается;

– помещения, выделенные для проведения мероприятий.

В интересах ЗИ о вооружении и военной технике защите подлежат:

– характеристики и параметры конкретных образцов вооружений и военной техники на всех этапах их жизненного цикла;

– научно-исследовательские, опытно-конструкторские и экспертные работы военно-прикладной направленности.

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

– о местоположении объекта;

– о предназначении, структуре объекта и режимах его функционирования;

– информация, циркулирующая в технических средствах, используемых на объекте;

– информация о разрабатываемых и эксплуатационных образцах вооружения, военной техники и технологии;

– информация о научно-исследовательских и опытно-конструкторских работах.

Задание 2. Для выбранного объекта защиты составить структурную модель защищаемой информации. Структурирование производится путем классификации защищаемой информации в соответствии с функциями, задачами и дальнейшей привязкой элементов информации к их носителям. Пример структурной модели приведен на рисунке 2.1.

Провести классификацию и структурирование информации в соответствии с функциями, задачами и структурой организации, в результате чего защищаемая информация должна быть представлена в виде отдельных элементов информации.

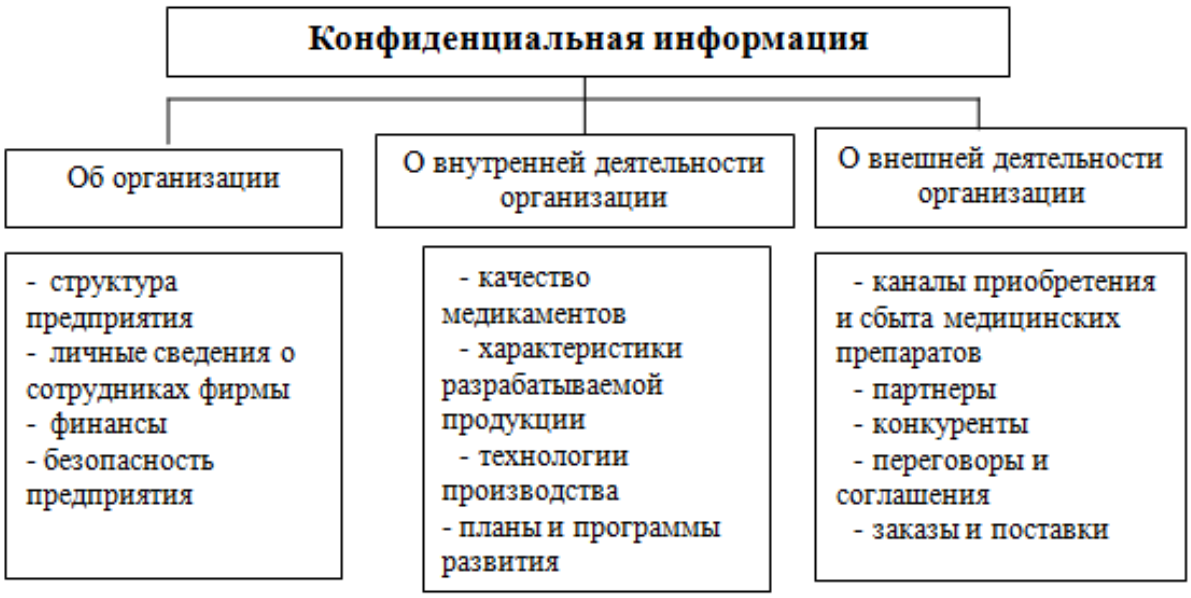

Рисунок 2.1 – Пример структурной модели конфиденциальной информации

2.3 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.

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 включает в себя:

– определение источников защищаемой информации,

– описание пространственного расположения основных мест размещения источников защищаемой информации,

– выявление путей распространения носителей защищаемой информации за пределы контролируемых зон,

– описание объекта защиты с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

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 инф-ции и определяются слабые места существующей системы защиты. Результаты моделирования отображаются в виде таблиц.

Задание 3. Провести анализ защищаемой информации и составить граф-структуру в соответствии со своим вариантом. Пример оформления граф-структуры приведен в таблице 2.3

Таблица 2.3 - Граф-структура защищаемой информации

№ п\п	Наименование источника информации	Гриф конфиденциаль-ности	Источник информации	Место нахождения источника информации
1	Структура предприятия	ДСП	Контракты, документы на бумажных носителях	Сейф с секретными документами, каб. №2
2	Личные сведения о сотрудниках фирмы	ДСП	Документы на бумажных носителях	Сейф с секретными документами, каб. №2
3	Финансы	ДСП	Документы на бумажных и электронных носителях, БД	Сейф с секретными документами, каб. №2. ПЭВМ каб.№3

2.4 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.

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 2.4).

Таблица 2.4 - Уровни конфиденциальности 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

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.

2.5 Определение задач и функций системы физической защиты

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 1.2.

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.

Рисунок 2.2 - Основные задачи системы физической защиты

Задание 4. Определить задачи и функции системы физической защиты в соответствии с вариантом.

2.6 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).

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.

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.

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.

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.

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.

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 2.3.

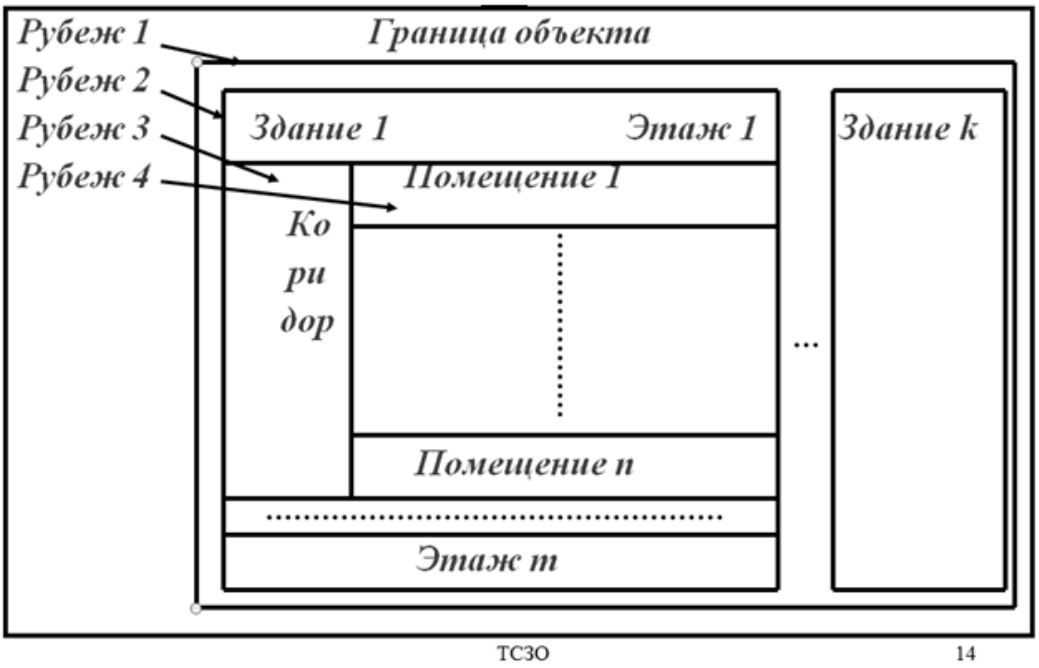

Рисунок 2.3 - Пример построения многорубежной защиты объекта

Задание 5. Сформулировать принципы системы защиты для своего варианта. Разработать план построения рубежей защиты заданного объекта.

2.7 Содержание отчета

1 Цель работы.

2 Задачи.

3 Описание объекта защиты, характеристика назначения объекта.

4 Разработка плана объекта защиты.

5 Построение пространственной модели объекта.

6 Построение структурной модели конфиденциальной информации.

7 Разработка граф-структуры защищаемой информации.

8 Определение категории защищаемой информации.

9 Определение задач и функций СФЗ. Оформление в виде таблицы.

10 Формулирование принципов построения СФЗ для указанного варианта.

11 Список использованных источников.

2.8 Контрольные вопросы

1 Дать определение физической защиты объекта информатизации.

6 Какие задачи решает система физической защиты?

7 Дать характеристику физических средств защиты объектов.

8 Назовите основные составляющие системы физической защиты объекта.

9 Назовите и дайте характеристику основных видов источников и носителей защищаемой информации.

10 Назовите классы секретности информации. По каким критериям определяется категория защищаемой информации?

11 Какие факторы необходимо учитывать при составлении граф-структуры защищаемой информации?

12 Охарактеризуйте этапы проектирования системы защиты объектов?

13 Назовите и кратко охарактеризуйте основные принципы построения системы защиты.

14 Что такое контролируемая зона, на какие типы подразделяются зоны, привести примеры.

15 Какие преимущества дает многозональность организации системы защиты?

16 Какие факторы определяют надежность системы безопасности?

17 Что такое адаптируемость системы безопасности?

18 В чем заключается принцип гибкости системы защиты объекта?

19 Дать определение и назвать средства контроль и управление доступом.

3 Лабораторная работа № 2. Разработка модели угроз защищаемого объекта

Цель. Построение модели угроз безопасности защищаемого объекта информатизации.

Задачи.

1) Определение перечня угроз безопасности объекта.
2) Анализ каналов утечки информации.
3) Построение модели угроз с учетом каналов утечки.
4) Разработка модели вероятного нарушителя.

3.1 Определение перечня угроз безопасности объекта

Угроза - потенциальная возможность совершения действий направленных на нарушение безопасности объекта.

Проявление угроз (фактор неопределенности):

- действие нарушителей;
- воздействие стихийных сил;
- сбои в работе средств СФЗ;
- воздействие субъективного фактора.

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых на объекте и условий расположения и эксплуатации объекта.

Для составления перечня угроз необходимо:

- определить перечень актуальных источников угроз;
- определить перечень актуальных уязвимостей;
- оценить взаимосвязь угроз, источников угроз и уязвимостей;
- определить перечень возможных атак на объект;
- описать возможные последствия реализации угроз.

Угрозы утечки информации по техническим каналам.

1) Угрозы утечки речевой (акустической) информации по техническим каналам.

2) Характеристика угроз перехвата видовой (графической) информации ограниченного доступа визуальнооптическими средствами.

3) Угрозы утечки информации ограниченного доступа по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка информации - неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и ее получения разведками.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Основные элементы описания угроз утечки информации по техническим каналам представлены на рисунке 3.1.

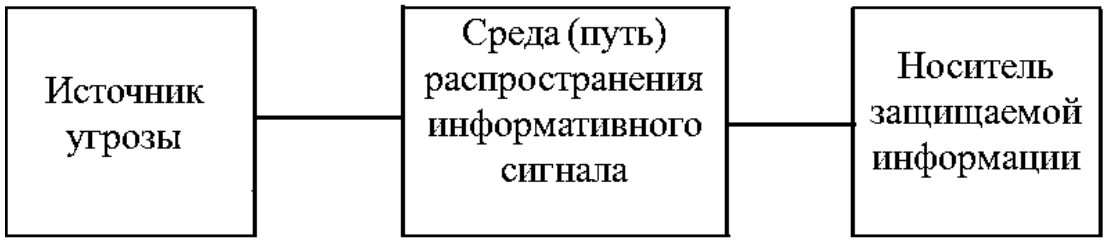

Рисунок 3.1 - Основные элементы угроз утечки информации

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Задание 1. Составить перечень угроз для заданного объекта по образцу таблицы 3.1.

Таблица 3.1 - Перечень угроз

№ угрозы	Источник угрозы	Среда распространения	Носитель информации

3.2 Анализ каналов утечки информации

Каналы утечки информации по физическим принципам можно классифицировать на следующие группы:

- акустические (включая и акустопреобразовательные);
- визуально-оптические (наблюдение, фотографирование);
- электромагнитные (в том числе магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители и т.п.).

При использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

– акустическое излучение информативного речевого сигнала;

– электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам, выходящими за пределы КЗ;

– виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

– несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

– воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

– побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;

– наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

– радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств;

– радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;

– радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

– прослушивание ведущихся телефонных и радиопереговоров;

– просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

– хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

Задание 2. Провести анализ потенциальных каналов утечки на указанном объекте. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 3.2.

Таблица 3.2 - Перечень потенциальных каналов утечки информации

Каналы утечки информации с объекта защиты			Место расположения
1.	Оптический канал	Окно со стороны проспекта	каб. №1
		Окно со стороны проспекта	каб. №2
		Окно со стороны проспекта	каб. №3
2.	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		Телефон	указать
		Розетки	указать
		ПЭВМ	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать
3.	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
4.	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

3.3 Моделирование угроз безопасности с учетом каналов утечки

Моделирование угроз безопасности информации предусматривает анализ способов её хищения, изменения, уничтожения с целью оценки наносимого ущерба. Моделирование угроз включает моделирование:

- способов физического проникновения;
- технических каналов утечки информации.

Возможные пути проникновения злоумышленника отмечаются на планах, схемах территорий, этажей помещений линиями. Результаты оформить в виде следующей модели, показанной в таблице 3.3.

Таблица 3.3 – Модель угроз защищаемого объекта

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Моделирование технических каналов утечки информации (ТКУИ) является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты. Целесообразно рассматривать каналы в статике и динамике. Статическое состояние характеризует пространственное состояние структурной модели, описывает состав и связи элементов канала утечки. Пространственная модель содержит описание положения канала утечки в пространстве: места расположения источника и приёмника сигналов. Ориентация вектора распространения носителя информации в канале утечки и его протяжённость структурную модель целесообразно представить в табличной форме. Пространственную – в виде графов на планах помещений.

Динамику канала утечки описывает **функциональная и информационная модель.** Функциональная модель характеризует режимы функционирования канала: это может быть интервал времени, в течении которого возможна утечка. Информационная модель содержит характеристики информации, утечка которой возможна по техническому каналу(количество и ценность).

Указанные модели объединяются и увязываются между собой в рамках комплексной модели канала утечки. В ней указываются интегрированные параметры утечки – источник информации, его вид, ист-к сигнала, среда распространения, протяжённость среды распространения, возможное место размещения приёмника сигнала, информативность канала, величина угрозы. Все выявленные потенциальные каналы утечки и их характеристики заносятся в таблицу 3.4.

Таблица 3.4 – Комплексная модель каналов утечки

№	Цена информации	Источник сигнала	Путь утечки	Вид канала	Оценка реальности	Величина угрозы/ранг

Оценка угроз информации в результате проникновения злоумышленника к источнику или в результате её утечки по ТКУИ проводится с учётом вероятности реализуемости рассматриваемого пути или канала, а также с учётом цены соответствующего элемента информации. Угроза безопасности информации выражается в величине ущерба при захвате её к злоумышленником, где - цена элемента информации - вероятность угрозы.

Задание 3. Построить модель угроз и комплексную модель каналов утечки информации для заданного объекта.

3.4 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.

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.

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.

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.

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.

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 3.2.

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

Рисунок 3.2 - Типовая модель нарушителя

Задание 4.

1) Провести анализ вероятных внешних и внутренних нарушителей.

2) Построить модель вероятного нарушителя (внешнего и внутреннего) на основе моделей угроз и утечки информации, а также граф-структуры защищаемой информации, разработанной в лабораторной работе № 1.

Задание 5. Обозначить на плане объекта (разработанного в лабораторной работе № 1) возможные пути проникновения нарушителя на территорию по образцу на рисунке 3.3.

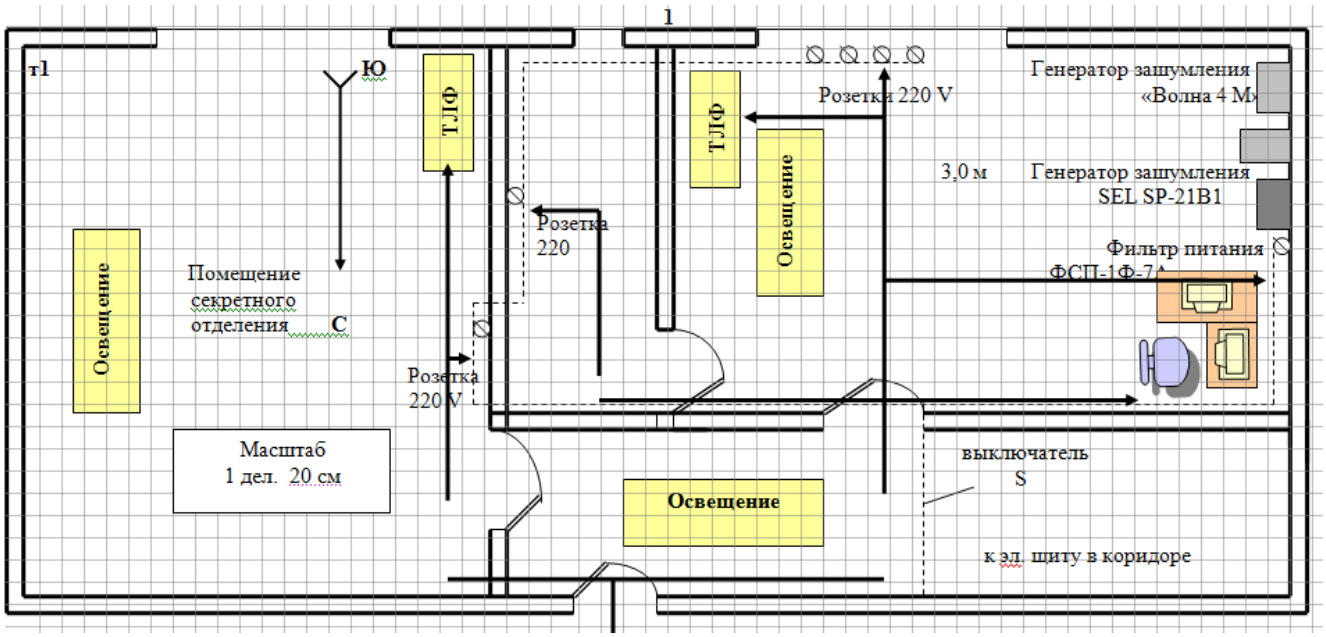

Рисунок 3.3 - Возможные пути проникновения нарушителя

3.5 Содержание отчета

1 Цель.

2 Задачи.

3 Составить перечень угроз и каналов утечки для заданного объекта.

4 Составить ранжированный перечень защищаемой информации.

5 Построить модель угроз и каналов утечки.

6 Построить модель вероятного нарушителя.

7 Построить план возможных путей проникновения нарушителя.

8 Сделать выводы о проделанной работе.

3.6 Контрольные вопросы

1 Что является исходными данными для проведения оценки и анализа угроз безопасности объектов?

2 Дать определение нарушителя, по каким критериям они классифицируются?

3 Дать определение технического канала утечки информации, назвать типы.

4 Дать определение носителя защищаемой информации, назвать типы.

5 Какие сведения включает пространственная модель каналов утечки?

6 Что такое формализованная и неформализованная модель нарушителя?

7 Перечислите цели и задачи вероятного нарушителя.

8 Какое оборудование относят к виброакустические каналам утечки информации?

9 Дать описание четырех категорий нарушителя.

10 Что представляет собой матрица угроз/средств защит и матрица вероятностей наступления угроз?

4 Лабораторная работа № 3. Моделирование мероприятий физической защиты объекта

Цель. Построение модели системы физической защиты заданного объекта.

Задачи.

1) Разработка функциональной структуры СФЗ.

2) Разработка топологической структуры СФЗ.

3) Разработка плана организационно-технических мероприятий по защите объекта.

Мероприятия по технической защите информации можно условно разделить на три направления: пассивные, активные и комбинированные.

Пассивная защита подразумевает обнаружение и локализацию источников и каналов утечки информации. Активная — создание помех, препятствующих съему информации. Комбинированная — сочетает в себе использование двух предыдущих направлений и является наиболее надежной. Однако пассивная и активная защиты уязвимы в некотором смысле. Например, при использовании исключительно пассивной защиты приходится проводить круглосуточный мониторинг, так как неизвестно, когда включаются средства съема, или теряется возможность использовать оборудование обнаружения при проведении деловой встречи. Активная защита может заметно осложнить ведение наблюдения за объектом, но есть вероятность использования ее вхолостую, не зная точно, есть ли наблюдение. Комбинированная защита позволяет устранить эти недостатки.

Основные методы инженерно-технической защиты.

1) Создание физических, электронных и других препятствий злоумышленнику на пути к носителям конфиденциальной информации.

2) Введение злоумышленника в заблуждение с помощью технических средств путем подготовки и распространения ложной информации.

3) Применение различных средств контроля несанкционированного доступа для выявления попыток реализации злоумышленником угроз безопасности информации.

4) Предупреждение должностных лиц и персонала предприятия о возникновении чрезвычайных ситуаций на объектах.

ТСФЗ по функциональному назначению подразделяют на следующие функциональные средства и системы:

– охранной сигнализации: средства обнаружения, система сбора и обработки информации;

– тревожно-вызывной сигнализации;

– контроля и управления доступом;

– оптико-электронного наблюдения и оценки обстановки;

– оперативной связи и оповещения;

– обеспечения электропитания и электроосвещения.

Классификация инженерно-технических средств защиты приведена на рисунке 4.1.

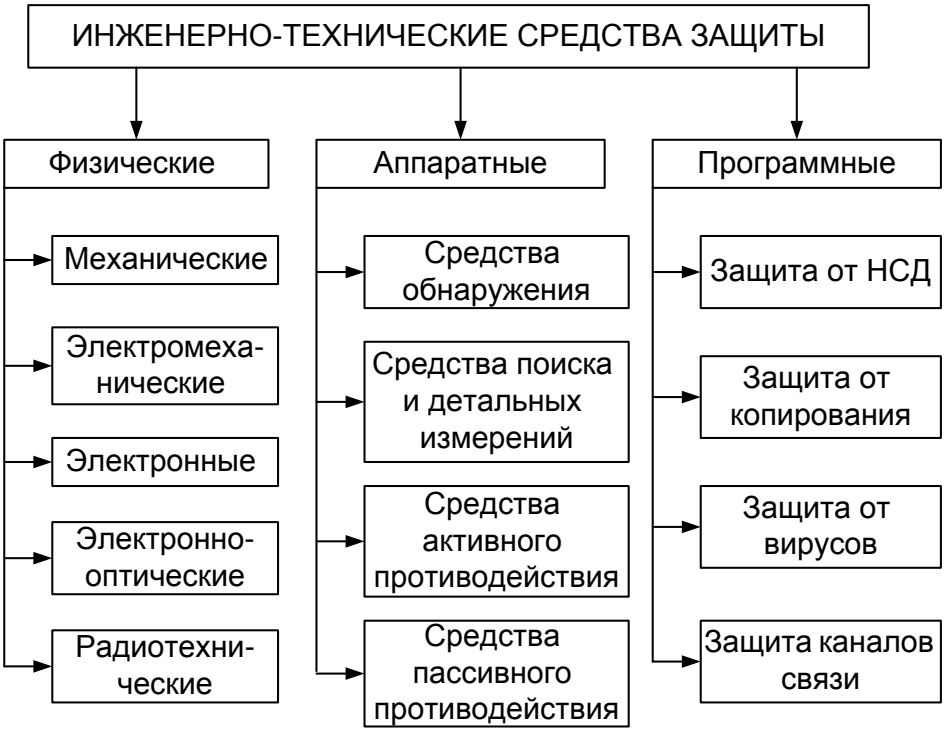

Рисунок 4.1 - Классификация инженерно-технических средств защиты

4.1 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).

Функции СФЗ показаны на рисунке 4.2.

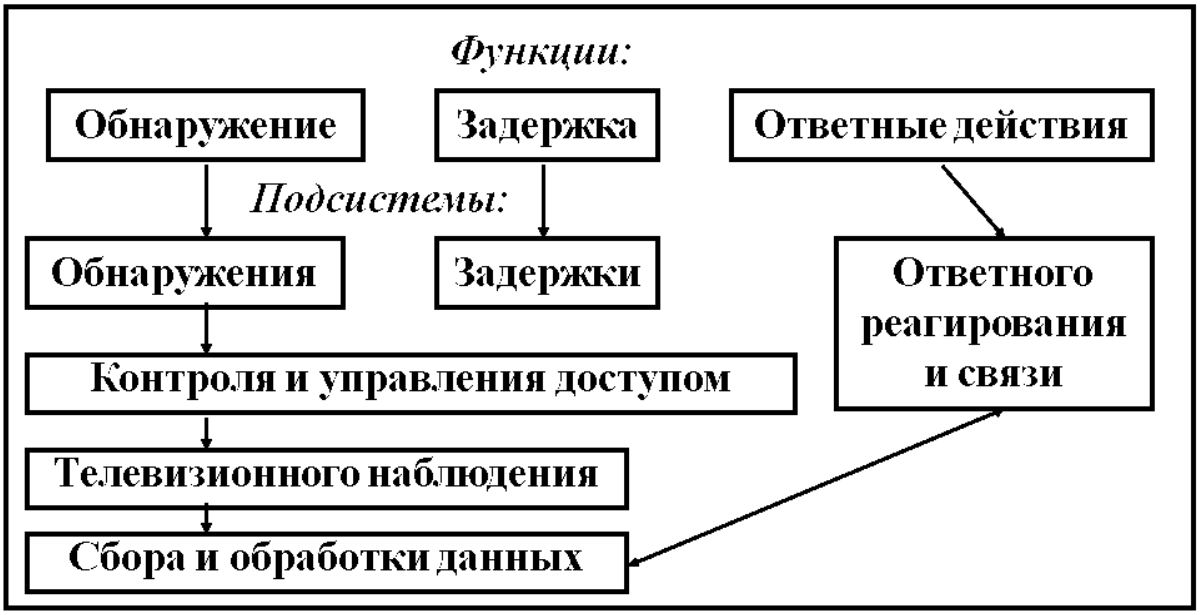

Рисунок 4.2 - Функции СФЗ

Задание 1. Построить функциональную структуру СФЗ заданного объекта. Разработать модель мероприятий физической защиты объекта в соответствии с моделями угроз и каналов утечки информации на заданном объекте, построенных в работе № 2.

4.2 Топологическая структура СФЗ объекта

Топологическая структура СФЗ объекта необходима для планирования и реализации рубежей охраны объекта на основе анализа контролируемых зон.

На плане охраняемого объекта выделяют зоны по степени значимости информации, как показано на рисунке 4.3.

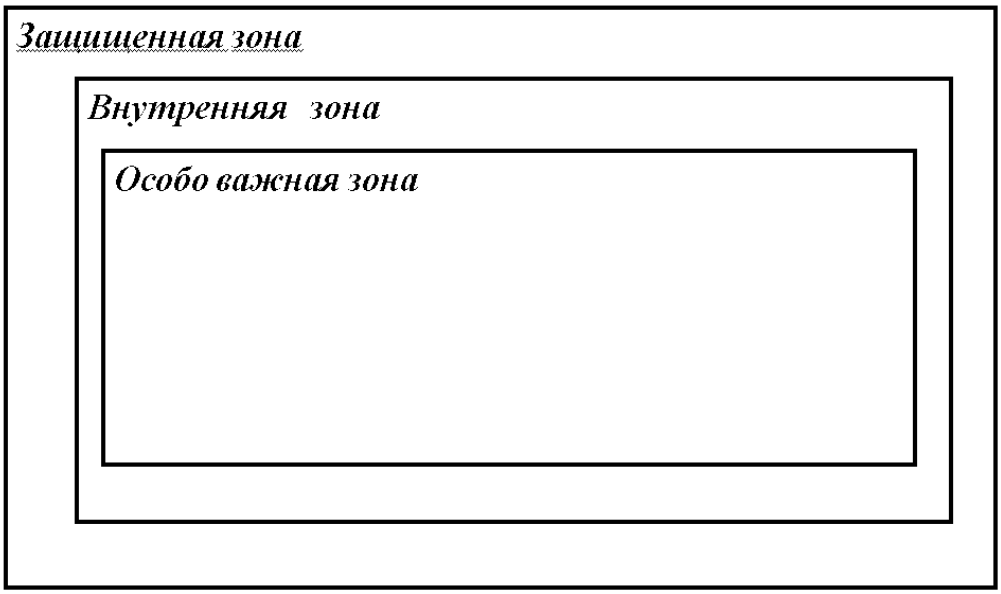

Рисунок 4.3 Ранжирование охраняемых зон объекта

Задание 2. В соответствии с граф-структурой защищаемой информации заданного объекта, созданной в лабораторной № 1, провести ранжирование зон защищаемого объекта и построить топологическую структуру СФЗ заданного объекта.

4.3 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.

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.

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).

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;

– 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.

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.

Задание 3. Составить план организационно- технических мероприятий по образцу таблицы 4.1.

Таблица 4.1 - План организационно технических мероприятий

№ п\п	Демаскирующий признак	Мероприятия по уменьшению (ослаблению) демаскирующих признаков
I. Организационные мероприятия		
1.	Прибытие сотрудников на службу в форменной одежде	1. Прибытие сотрудников на службу в форменной одежде другого ведомства 2. Проведение совещаний и переподготовки сотрудников других ведомств
3.	Перемещение сотрудников	1. Разграничение доступа сотрудников в различные помещения 2. Организация пропускного режима
4.	Готовая продукция	1. Разграничение доступа сотрудников в склад при вывозе продукции за пределы предприятия
5.	Отходы производства	1. Сбор и утилизация отходов производства 2. Уничтожение отходов делопроизводства
II. Технические мероприятия		
1.	Излучение ПЭВМ	1. Организация работы системы зашумления 2. Установка в ПЭВМ генераторов зашумления 3. Персонификация доступа в систему 4. Программная защита системы ПЭВМ 5. Плановые (внеплановые) проверки ПЭВМ
2.	Телефонная связь	1. Организация работы внутренней АТС 2. Запись переговоров сотрудников по телефонам 3. Закрытие каналов связи
3.	Строительные конструкции здания	1. Нанесение на стекла пленки поглощающей ИК - излучение 2. Установка системы виброакустического зашумления стекол и строительных конструкций 3. Специальная проверка персонала обслуживающего смежные помещения

4.4 Содержание отчета

3 Цель.

4 Задачи лабораторной работы.

3 Функциональная структура СФЗ.

4 Топологическая структура СФЗ.

5 План организационно-технических мероприятий по защите объекта.

6 Выводы по работе.

4.5 Контрольные вопросы

1 Назвать основные методы инженерно-технической защиты.

2 Какие типы структур необходимо построить для создания модели системы физической защиты объектов?

3 На какие функциональные средства и системы подразделяют технические средства физической защиты?

4 Что включает в себя функциональная структура системы физической защиты?

5 Для чего необходимо строить топологическую структуру системы физической защиты объекта?

6 Дать определение понятий постоянной и временной контролируемых зон защищаемого объекта.

7 На какие группы подразделяются технические средства, используемые для передачи, обработки и хранения конфиденциальной информации (ОТСС)?

8 На какие группы подразделяются вспомогательные технические средства и системы (ВТСС)?

9 Какие пункты включает в себя план организационно технических мероприятий защиты объекта?

10 Назовите средства сокрытия информации о защищаемом объекте.

5 Лабораторная работа № 4. Разработка структурной схемы и выбор оборудования системы физической защиты объекта

Цель. Разработка плана размещения физических средств защиты и формирование спецификации оборудования.

Задачи.

1) Разработка структурной схемы системы защиты объекта.
2) Выбор приборов и оборудования СФЗ для заданного объекта.
3) Разработка спецификации средств СФЗ.
4) Разработка плана размещения средств СФЗ.

5.1 Разработка структурной схемы системы защиты объекта

При проектировании новой системы следует решить, как наилучшим образом интегрировать людей, процедуры и технические средства для решения задач СФЗИ. Первичными функциями СФЗИ являются обнаружение нарушителя, его задержка, а также реагирование персонала службы безопасности. Важно отметить, что для эффективной задержки должно произойти обнаружение. Приоритетная цель системы - защитить критичные ресурсы от хищения или диверсии со стороны злонамеренного лица. Для того чтобы система эффективно выполняла эту задачу, должно иметь место оповещение о нападении (задержка), что позволит самим силам реагирования прервать или остановить действия нарушителя.

Современный подход к обеспечению безопасности предполагает реализацию трех последовательных рубежей защиты. Обнаружение, задержка и реагирование - необходимые функции эффективной СФЗИ. Они должны выполняться в указанном порядке в течение времени меньшего, чем время, необходимое для достижения нарушителем его задачи.

Функции СФЗ.

1) Обнаружение: использование извещателей охранной сигнализации; видеокамеры с детекторами движения.

2) Задержка: турникеты и ограждения на проходной; таблички с информацией о ведущемся видеонаблюдении.

3) Реагирование: использование системы оповещения; автоматическое реагирование системы; вызов уполномоченных органов защиты.

Структура СФЗ представлена на рисунке 5.1.

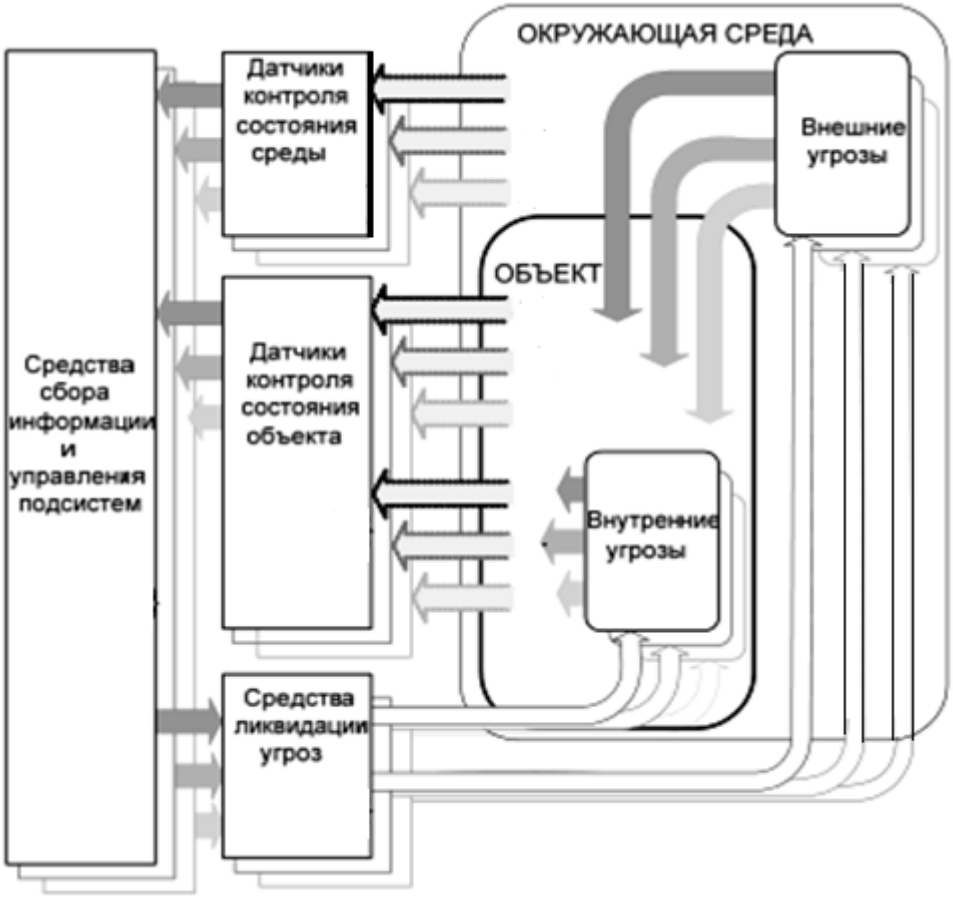

Рисунок 5.1 - Структура СФЗ

5.2 Выбор приборов и оборудования СФЗ для заданного объекта

Средства задержания предназначены для решения следующих задач:

1. Обеспечения условий для задержания нарушителей при вторжении на охраняемый объект на время, необходимое для организации обороны объекта.

2. Задержания нарушителя при проникновении на охраняемый объект на время, необходимое для его нейтрализации силами охраны.

3. Обеспечения условий для санкционированного прохода на охраняемый объект и выхода за его пределы без дополнительных затрат на преодоление рубежей охраны.

4. Обеспечения условий для предотвращения несанкционированного вывоза (ввоза) имущества.

5. Предотвращения (усложнения) наблюдения нарушителем за охраняемым объектом.

Физическими барьерами называется комплекс заградительных инженерных сооружений и средств, решающих задачи как самостоятельно, так и в совокупности с другими составными частями системы инженерных средств физической защиты.

Самостоятельные задачи:

а) задержание нарушителя при проникновении на охраняемый объект на время, необходимое для его нейтрализации силами охраны;

б) предотвращение (усложнение) наблюдения за охраняемым объектом. Правила установки:

- основное заграждения,
- предупредительное заграждения,
- заградительные инженерные средства,
- ворота, калитки, шлюзы.

Совместные задачи - обеспечение условий для:

- задержания нарушителей при вторжении на охраняемый объект на время, необходимое для организации обороны объекта;
- санкционированного прохода на охраняемый объект и выхода за его пределы без дополнительных затрат на преодоление рубежей охраны;
- предотвращения несанкционированного вывоза (ввоза) имущества.

5.3 Периметральные средства обнаружения

Функции обнаружения выполняют периметральные датчики. Работа периметральной сигнализации базируется на законах физики и химии и отличается применением чувствительных датчиков и элементов различного типа. Многообразие применяемых периметральных средств обнаружения объясняется работой в самых разных условиях. На рисунке 5.2 приведена классификация периметральных средств обнаружения.

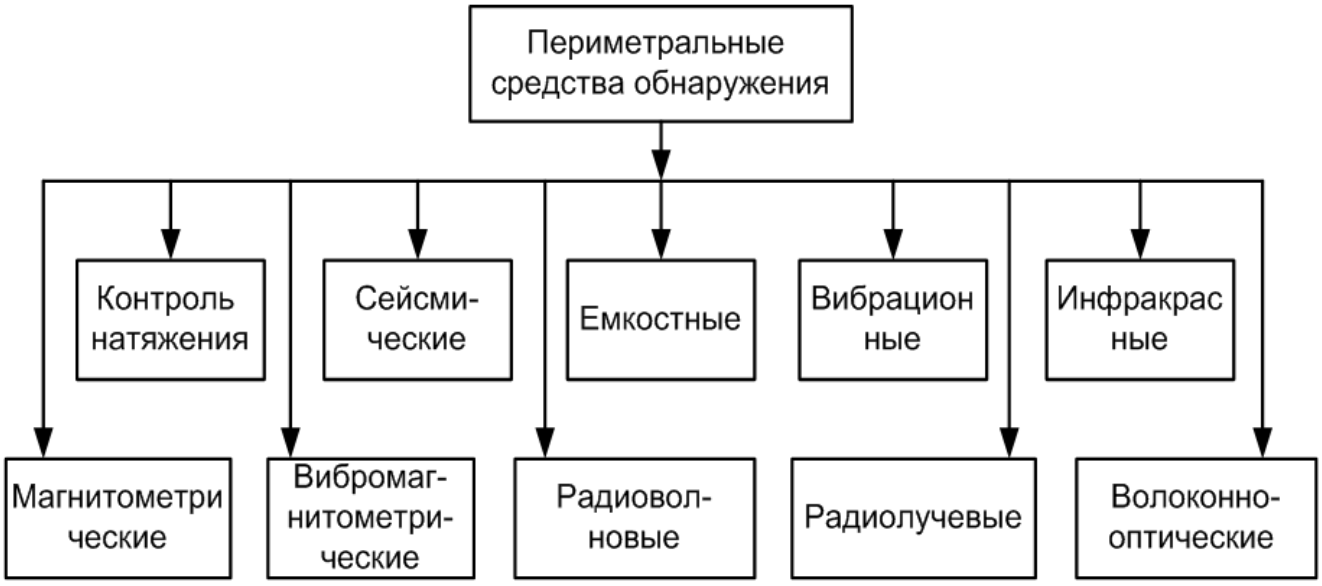

Рисунок 5.2 - Классификация периметральных средств обнаружения

Общие требования к периметральным системам.

1) Возможность раннего обнаружения нарушителя — еще до его проникновения на объект.

2) Точное следование контурам периметра, отсутствие “мертвых” зон.

3) По возможности скрытая установка датчиков системы.

4) Независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т.д.).

5) Невосприимчивость к внешним факторам “нетревожного” характера — индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы.

6) Устойчивость к электромагнитным помехам — грозовые разряды, источники мощных электромагнитных излучений и т.п.

Периметральные средства обнаружения классифицируются по физическому принципу:

– электромеханическое средство обнаружения, где чувствительный элемент натянутые нити из проволоки на концах которых находятся датчики, малейшее изменение в размере нити, обрыв и перекусывание приведет к тревожному сигналу;

– вибрационное средство обнаружения, где чувствительный элемент трибоэлектрические датчики вибрации и система точечных электромагнитных (пьезоэлектрических) датчиков вибраций, действие которых основано на колебании полотна ограждений (например, когда проделываются отверстия для лаза или перелазают через ограждение);

– емкостное средство обнаружения, когда изменяется емкость чувствительного элемента (проделывание отверстия, перелезание), что приводит к срабатыванию сигнала тревоги;

– индуктивные средства обнаружения, когда изменяется индуктивность петли чувствительного элемента в следствии обрыва, раздвижения, разрезания проводов, подается соответствующий сигнал о тревоге;

– радиолучевое средство обнаружения, работа основана на разнесении СВЧ-передатчика и приемника, когда изменяется уровень принимаемого сигнала между приборами из-за движения постороннего предмета или нарушителя. при эксплуатации простейшего проводноволнового средства обнаружения применяется система параллельных проводов, когда по ним происходит передача и прием излучения, а изменения в уровне воспринимаемого сигнала, создаваемые движением нарушителя рядом с системой проводов приведет к срабатыванию тревожного сигнала;

– магнитометрическое средство обнаружения, представляет систему проводов (датчиков), обнаруживающую изменение магнитного поля в случае перемещения через неё металлического предмета;

– сейсмическое средство обнаружения, представляет из себя систему геофонных датчиков смонтированных непосредственно в грунте, их действия основаны на сейсмических колебаниях грунта, вызываемых подвижкой почвы;

– оптикоэлектронное средство обнаружения, когда передатчик и приемник разнесены друг от друга и формируется инфракрасный луч, малейшее прерывание свечения лучей нарушителем приведет к срабатыванию охранной системы.

5.4 Задание к лабораторной работе

Задание 1. В соответствии с функциями СФЗ и опираясь на результаты анализа угроз и каналов утечки информации на заданном объекте, сделанных в предыдущих лабораторных работах, необходимо построить структурные схемы:

– подсистемы обнаружения: датчики, извещатели;

– подсистемы задержки: ограждения, замки и т.д.;

– подсистемы реагирования: сигнализация, индикация, оповещения, организация сил охраны.

Затем разработать комплексную структурную схему системы физической защиты.

Задание 2. Разработать функциональную спецификацию системы физической защиты по образцу таблицы 5.1.

Таблица 5.1 - Функциональная спецификация системы физической защиты

№	Функция	Средство
1	Обнаружение нарушения периметра	Периметральный датчик
2	Обнаружение движущегося объекта	Датчик движения
3	Задержка прохода	Турникет

Задание 3. Осуществить выбор необходимых приборов и оборудования для обеспечения функций СФЗ. Составить спецификацию.

Построить модель защиты информации от утечки по техническим каналам по образцу таблицы 5.2.

Таблица 5.2 - Модель защиты информации от утечки по техническим каналам

№ п\п	Место установки	Позиционное место установки устройств съема информации	Тип (индекс) устройства съема информации	Способ применения	Технический канал закрытия утечки информации
1.	Рабочий стол руководителя объекта защиты	С1:5	Генератор шума «Гром ЗИ – 4»	Постоянно	Радиоэлектронный
2.	ПЭВМ кабинета №3	V1:13	Генератор шума «ГШ-К-1000М»	Постоянно	Радиоэлектронный
3.	Помещение секретного отделения	Т6	Генератор шума «Купол-W-ДУ»	Постоянно	Радиоэлектронный
4.	Розетка 220 В. Кабинет руководителя объекта защиты	Х1:10	Генератор шума «SEL SP-41/C»	По решению руководства	Радиоэлектронный

Задание 4. Разработать план размещения приборов и оборудования на заданном объекте.

5.5 Содержание отчета

1 Цель.

2 Задачи лабораторной работы.

3 Построение структурных схем: подсистемы обнаружения; подсистемы задержки; подсистемы реагирования.

4 Структурная схема СФЗ.

5 План размещения приборов и оборудования на заданном объекте.

6 Выводы по работе.

5. 6 Контрольные вопросы

1 Назвать основные составляющие структуры СФЗ и дать краткую характеристику.

2 Какие задачи решает подсистема задержания нарушителя?

3 Какие физические средства используют для реализации задач подсистемы задержания?

4 Что такое физический барьер?

5 Дать определение и перечислить задачи системы контроля и управления доступом.

6 Назвать задачи и функции подсистемы обнаружения.

7 Дать определение и назвать средства контроля и управления доступом. Перечислить решаемые задачи.

8 Что такое периметральная защита, какие средства её реализуют?

9 Назовите основные классы периметральных датчиков. На чем основан их принцип работы.

10 Назовите средства реагирования и меры по их организации.

Список использованных источников

1 Андрианов, В. И. Устройства для защиты объектов и информации: справочное пособие / В. И. Андрианов, А. В. Соколов- 2-е изд., перераб. и доп.- М.: АСТ ; СПб. : Полигон, 2000. - 256 с.

2 Волхонский, В.В. Системы охранной сигнализации/ В.В. Волхонский. – СПб: Экополис и культура, – 2000. – 164 с.

3 Волхонский, В.В. Устройства охранной сигнализации/ В.В. Волхонский 2-е изд., доп. и перераб. – СПб.: Экополис и культура, – 2000. – 312 с.

4 Гришина, К.В. Организация комплексной системы защиты информации/ К.В. Гришина. - Таганрог: изд -во ТРТУ , 2003. – 321 с.

5 Корнюшин, П.Н. Информационная безопасность: учебное пособие/ П.Н. Корнюшин, С.С. Костерин. – Владивосток: ДВГУ, 2005. - 345 с.

6 Меньшаков, Ю.К. Защита объектов и информации от технических средств разведки: учеб. пособие / Ю. К. Меньшаков. – М.: РГГУ, 2002. – 296.с.

7 Петраков, А. В. Основы практической защиты информации: учеб. пособие / А. В. Петраков.- 4-е изд., доп. - М.: СОЛОН-Пресс, 2005. - 384 с.

8 Романец, Ю.В. Защита информации в компьютерных системах и сетях/ Ю.В. Романец, П.А.Тимофеев. – М.: Радио и связь, 2000. – 328 с.

9 Садердинов, А. А. Информационная безопасность предприятия: учеб. пособие для вузов / А. А. Садердинов, В. А. Трайнев, А. А. Федулов.- 2-е изд. - М.: Дашков и К, 2005. - 336 с.

10 Соколова, С.П. Интеллектуальные системы охраны/ С.П. Соколова, А.Д. Джангозин, В.Н. Боркин. – Алматы: Академия МВД РК, – 2000. – 204 с.

11 Торокин, А.А. Инженерно-техническая защита информации: учебное пособие/ А.А. Торокин. – М.: Гелиос АРВ, 2005. - 960с.

12 Хорев, А.А. Защита информации от утечки по техническим каналам/ А.А. Хорев. – М.: Гостехкомиссия России, 1998. – 320 с.

13 Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. – М.: Междунар. отношения, 2000. – 400 с.