Министерство образования и науки Российской Федерации

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

Кафедра вычислительной техники и защиты информации

Е.В. Бурькова

ФИЗИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Рекомендовано ученым советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по программам высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург
2017

УДК 004.891
ББК 32.965
Б 91

Рецензент – доктор технических наук, профессор В.И. Чепасов

Бурькова Е.В.

Б 91 Физическая защита объектов информатизации: учебное пособие / Е.В. Бурькова; – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2017. – 157 с.

ISBN 978-5-7410-1697-8

В учебном пособии представлены теоретические сведения о структуре, составе и основных задачах системы физической защиты объектов, рассмотрены вопросы категорирования объектов защиты, классификации физических средств защиты подсистем обнаружения, задержки. Учебное пособие содержит практические задания и вопросы для самопроверки.

Учебное пособие предназначено для студентов направления подготовки 10.03.01 Информационная безопасность при изучении курса «Физические средства защиты объектов информатизации».

УДК 004.891
ББК 32.965

ISBN 978-5-7410-1697-8

Содержание

Введение

В современных условиях глобальной информатизации общества, практически все объекты экономики, а также объекты социальной структуры нуждаются в комплексной защите от угроз терроризма, чрезвычайных ситуаций, стихийных бедствий и угроз, исходящих от различного рода нарушителей. С каждым годом угрозы безопасности видоизменяются, повышается вероятность реализации киберугроз, нарушители становятся более осведомленными и технически подготовленными. При этом защищаемые объекты также развиваются; в качестве объектов защиты на них выступает персонал, информация, хранящаяся в базах данных, передаваемая по сетям, материальные и информационные активы организаций. Задача организации контроля физического доступа к защищаемым ресурсам становится первоочередной задачей политики безопасности любого объекта.

Системы физической защиты представляют собой совокупность физических, инженерно-технических, организационных мероприятий и действий охранных подразделений, предназначенных для защиты объекта от несанкционированных действий нарушителя.

Для решения задач проектирования системы физической защиты первоочередной задачей является обследование защищаемого объекта. В ходе обследования выясняются следующие вопросы:

- площадь территории объекта;
- количество зданий;
- количество локальных зон;
- ценность защищаемых ресурсов;
- месторасположение защищаемых ресурсов в структуре объекта;
- категория объекта по различным критериям (техническая укрепленность, пожарная безопасность, значимость объектов по функционально-отраслевым признакам);
- анализ близлежащих объектов и другие.

Выбор средств физической защиты объектов производится в соответствии с требованиями нормативно-правовых документов. В число таких документов входят:

− Р 78.36.007-99 «Выбор и применение средств охранно-пожарной сигнализации и средств технической укрепленности для оборудования объектов. Рекомендации»;

− РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств»;

− СП 132.13330.2011 «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования. Свод правил»;

− ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации».

Необходимо учитывать функционально-отраслевую значимость объекта, которая определяет виды потенциальных потерь при реализации угроз: политические потери, людские потери, экономические, социально-культурные, экологические и т.д. В этой связи, при разработке систем физической защиты принимают во внимание нормативно-правовые документы определенной отрасли экономики или социальной сферы.

Основной целью данного учебного пособия является рассмотрение теоретических основ физической защиты объектов информатизации, включающих обследование защищаемых объектов, анализ угроз безопасности, формирование требований к СФЗ, состава СФЗ, обзор и критерии выбора средств физической защиты. Учебное пособие предназначено для студентов, обучающихся по программам высшего образования по направлению подготовки «Информационная безопасность».

Основные понятия и определения

Безопасность объекта – состояние защищенности от внутренних и внешних угроз, обеспечивающее заданное функционирование объекта, не допуская диверсий, аварий, ситуаций, опасных для людей и окружающей среды.

Гибкость защиты – возможность оперативно изменять меры защиты.

Датчики (извещатели) – средства обнаружения.

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

Достоверность информации – показатель качества информации, означающий её полноту и общую точность.

Доступ - проход (проезд) в охраняемые зоны объекта предприятия.

Доступность информации - состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Задержка – замедление продвижения нарушителя.

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

Идентификатор доступа - демаскирующий признак субъекта и объекта, по которому принимается решение о доступе.

Извещателъ охранный (пожарный) - техническое средство ОПС для обнаружения проникновения, пожара, попытки проникновения или физического воздействия, превышающего нормированное значение, а также формирования извещения о проникновении (пожаре).

Извещение - сообщение о контролируемых изменениях состояния охраняемого объекта или технического средства ОПС и передаваемое с помощью электромагнитных, электрических, световых, звуковых сигналов.

Информационный портрет объекта защиты - описание объекта защиты в виде структуры его информационных элементов.

Источник информации – субъекты и объекты, от которых может быть получена информация с характеристиками, позволяющими оценить ее достоверность.

Источник угрозы безопасности информации - это субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации

Комплекс охранно-пожарной сигнализации - совокупность совместно действующих технических средств охранной, пожарной и (или) охранно-пожарной сигнализации, установленных на охраняемом объекте и объединенных системой инженерных сетей и коммуникаций.

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.

Контролируемая зона – часть пространства, в которой обеспечивается контроль безопасности информации.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

Многозональность физической защиты – разделение пространства, в которой находятся источники защищаемой информации, на зоны, уровень защиты информации в которых соответствует ее ценности.

Многорубежность физической защиты – наличие на пути распространения источников угроз преград, уменьшающих энергию источников угроз и увеличивающих время их продвижения к цели.

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

Надежность защиты информации предусматривает обеспечение требуемого уровня ее безопасности независимо от внешних и внутренних факторов, влияющих на безопасность информации.

Нарушитель — лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, пользователя, владельца, а также лицо, оказывающее ему содействие в этом.

Непрерывность физической защиты – постоянная готовность системы защиты к нейтрализации угроз.

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.

Оповещатель охранно-пожарный - техническое средство охранной, пожарной или охранно-пожарной сигнализации, предназначенное для

оповещения людей, находящихся на удалении от охраняемого объекта, о проникновении (попытке проникновения) или пожаре.

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

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

Охраняемый объект (ОО) - объект, охраняемый подразделениями охраны и оборудованный действующими техническими средствами охранной, пожарной или охранно-пожарной сигнализации.

Охраняемая зона - часть охраняемого объекта, контролируемая одним шлейфом ОПС или совокупностью шлейфов.

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

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

Пожарная сигнализация - получение, обработка, передача и представление в заданном виде потребителям при помощи технических средств информации о пожаре на охраняемых объектах.

Полномочие реагирования - полномочие, предоставляемое для реагирования по сигналу тревоги с охраняемой зоны с ответственностью за принятие необходимых мер.

Прибор приемно-контролъный охранный (охранно-пожарный) (ППКО, ППКОП) - техническое средство охранной или охранно-пожарной сигнализации для приема извещений от извещателей (шлейфов сигнализации) или других приемно-контрольных приборов, преобразования сигналов, выдачи извещений для непосредственного восприятия человеком, дальнейшей передачи извещений и включения оповещателей.

Пункт централизованной охраны - диспетчерский пункт для централизованной охраны ряда рассредоточенных объектов от проникновения

нарушителя и пожара с использованием систем передачи извещений о проникновении и пожаре.

Равнопрочность рубежа защиты - отсутствие в рубеже защиты участков, прочность которых ниже допустимого значения.

Регламентация – установление временных, территориальных и режимных ограничений в деятельности сотрудников организации и работе технических средств, направленных на обеспечение безопасности объекта.

Рубеж сигнализации - шлейф или совокупность шлейфов, контролирующих охраняемые зоны на пути движения нарушителя к материальным ценностям охраняемого объекта и имеющих выход на отдельный номер пульта централизованного наблюдения (ПЦН).

Рубеж охраны - совокупность охраняемых зон, контролируемых рубежом сигнализации.

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

Система охранно-пожарной сигнализации — совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемых объектах и (или) пожара на них, передачи, сбора, обработки и представления информации в заданном виде.

Система передачи извещений (СПИ) - совокупность совместно действующих технических средств для передачи по каналам связи и приема в пункте централизованной охраны извещений о проникновении на охраняемые объекты и (или) пожаре на них, служебных и контрольно-диагностических извещений, а также для передачи и приема команд телеуправления.

Система тревожной сигнализации - электрическая установка, предназначенная для обнаружения и сигнализации о наличии опасности**.**

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

Тревога - предупреждение о наличии опасности или угрозы для жизни, имущества или окружающей среды.

Угроза – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности защищаемого объекта.

Уязвимость - это слабое место в системе защиты объекта, обусловливающее возможность реализации угроз безопасности.

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

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

Ценность информации - ценность информационного актива, характеризуется величиной потерь, которые понесёт Организация в том случае, если угроза будет реализована.

Шлейф охранной (пожарной, охранно-пожарной) сигнализации - электрическая цепь, соединяющая выходные цепи охранных (пожарных, охранно-пожарных) извещателей, включающая в себя вспомогательные (выносные) элементы (диоды, резисторы, конденсаторы и т. п.) и соединительные провода, предназначенные для передачи на приемно-контрольный прибор извещений о проникновении, попытке проникновения, пожаре и неисправности, а в некоторых случаях и для подачи электропитания на извещатели.

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

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

1 Сущность и задачи физической защиты объектов информатизации

1.1 Анализ структуры физической защиты

Системы физической защиты представляют собой совокупность физических, инженерно-технических, организационных мероприятий и действий охранных подразделений, предназначенных для защиты объекта от несанкционированных действий нарушителя.

Цель физической защиты – это обеспечение заданного уровня безопасности объекта путем предотвращения несанкционированного доступа на объект физических лиц, транспортных средств и грузов, обнаружения и задержки нарушителей, предотвращения диверсий и чрезвычайных ситуаций.

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.

Структура и состав системы физической защиты формируется на основе данных обследования объекта защиты, в результате которого определяется категория объекта, величина потенциального ущерба и требования по организации системы защиты [9].

В целях защиты территории и объектов предприятия решением его руководителя создается система физической защиты, 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 [23].

В соответствии с задачами система физической защиты может быть представлена в виде структуры, состоящей из подсистем: обнаружения, задержки и реагирования (нейтрализации угроз). Структурная схема СФЗ по решаемым задачам показана на рисунке 1.1.

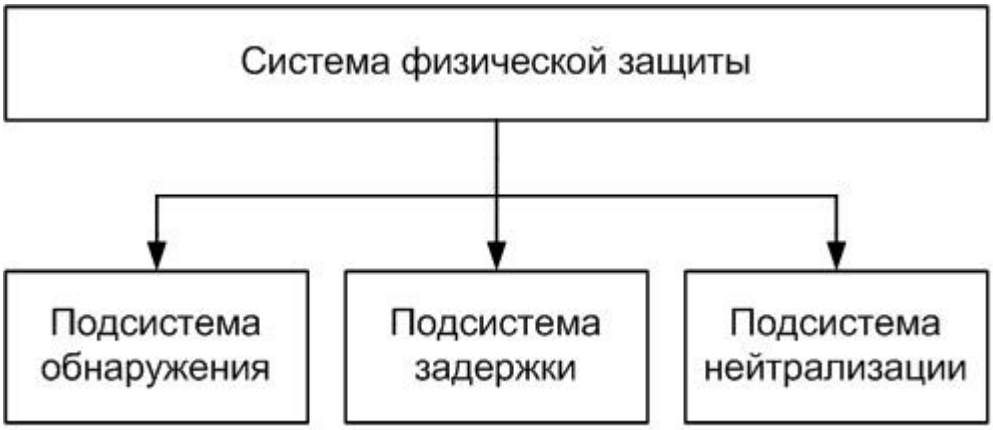


Рисунок 1.1. – Структурная схема СФЗ по решаемым задачам

Каждая из подсистем может быть реализована организационными мероприятиями, комплексом технических средств защиты и специальными подразделениями охраны. Подсистема обнаружения включает в себя охранные извещатели, тревожную сигнализацию, систему видеонаблюдения, контрольно-пропускные пункты. Подсистема задержки включает такие средства как физические барьеры (ограждения, КПП, двери, замки), СКУД и т.д. Подсистема нейтрализации угроз реализуется подразделениями охраны [38].

Система физической защиты в соответствии с определением, выполняемыми функциями, может быть представлена в виде совокупности

инженерно-технических, организационных мероприятий и действий подразделений охраны. Структура СФЗ по составу компонентов представлена на рисунке 1.2.

Рисунок 1.2 – Структура СФЗ по составу компонентов

Физические барьеры имеют в своем составе заграждения различных видов; ворота, калитки, шлюзы; двери, замки; блокирующие средства (шлагбаумы, противотаранные устройства, барьеры безопасности и т.д.).

Технические средства включают достаточно сложные подсистемы:

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

− системы пожарной сигнализации;

− тревожно-вызывной сигнализации;

− контроля и управления доступом;

− оптико-электронного наблюдения и оценки обстановки;

− оперативной связи и оповещения (в том числе средства проводной связи и радиосвязи);

− защиты информации;

− обеспечения электропитания и охранного электроосвещения.

Важное место в системе защиты объекта занимают организационные мероприятия, которые должны быть разработаны в виде документов и утверждены руководителем объекта [24]. Документы должны включать положение о службе безопасности, положение о внутриобъектовом режиме, инструкцию о пропускном режиме, план охраны объекта, план проверки технического состояния и работоспособности средств ФСЗ.

1.2 Принципы физической защиты объектов информатизации

При проектировании системы физической защиты объекта информатизации необходимо определить обязательные принципы, которые обеспечивают эффективную защиту. Принципы физической защиты являются основой для выбора методов и средств защиты. К ним относятся следующие:

− непрерывность;

− целенаправленность;

− конкретность;

- активность;
- надежность;
- комплексность;
- гибкость;
- скрытность;
- экономичность;
- многозональность;
- многорубежность;
- равнопрочность рубежа контролируемой зоны;
- ограниченный доступ к элементам системы защиты;
- адаптируемость системы защиты к новым угрозам;
- согласованность системы защиты с другими системами организации [29, 38].

Непрерывность физической защиты определяет постоянную готовность системы защиты к нейтрализации угроз, то есть при неизвестных заранее месте и времени реализации угроз безопасности нет перерывов в работе системы защиты, нет отказов или сбоев. Непрерывность защиты перекликается с понятием надежности работы системы защиты.

Надежность защиты подразумевает обеспечение требуемого уровня безопасности объекта независимо от внешних и внутренних факторов. Надежность защиты обеспечивается при условии безотказной работы сил и средств системы защиты. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя. Ущерб от неисправности технических средств защиты может быть очень высоким, равным цене информации. Ложные срабатывания средств защиты при отсутствии угрозы менее опасны, однако они способствуют ослаблению бдительности персонала охраны.

Целенаправленность защиты предусматривает сосредоточение усилий по предотвращению угроз наиболее ценного объекта защиты либо носителя информации.

Конкретность - защите подлежат конкретные данные, объективно нуждающиеся в охране, утрата которых может причинить организации определенный ущерб.

Активность защиты обеспечивается прогнозированием угроз и созданием превентивных мер по их нейтрализации.

Комплексность защиты заключается в применении комплекса мероприятий и средств защиты для обеспечения безопасности объекта, при котором недостатки одних средств и мер компенсируются достоинствами других.

Гибкость защиты необходима в связи с тем, что со временем все больше деталей системы защиты становится известными большему числу сотрудников и могут стать доступны нарушителю. Гибкость защиты предполагает изменять меры защиты в определенных случаях, или заменять одни меры на другие. Гибкость защиты обеспечивается многообразием способов и средств физической защиты объекта.

Скрытность защиты информации необходима, так как чем выше скрытность, тем больше неопределенность исходных данных у нарушителя и тем меньше у него возможностей по добыванию информации.

Экономичность защиты означает, что затраты на реализацию защиты не должны превышать возможный ущерб от реализации угроз.

Многозональность предусматривает разделение территории предприятия, здания на отдельные контролируемые зоны, в каждой из которых обеспечивается уровень безопасности в соответствии с ценностью информации, хранящейся в ней. Многозональность позволяет уменьшить расходы на средства защиты, так как в различных зонах будет реализована защита разной стоимости. Зоны могут быть независимыми, пересекающимися, вложенными.

Независимые зоны создаются для зданий и помещений, в которых выполняются существенно отличающиеся по уровню доступа работы, либо хранятся информационные или материальные ценности различной стоимости.

Пересекающиеся зоны характерны для таких мест объекта, к которым одновременно предъявляются повышенные требования к безопасности, и с другой стороны в нее имеют доступ многие сотрудники. Примером служит приемная руководителя учреждения, уровень безопасности должен быть выше, чем в коридоре, но его нельзя обеспечить таким же высоким, как в кабинете руководителя.

Вложенные зоны наиболее распространены, так как позволяют экономно обеспечить требуемый уровень безопасности. Безопасность n-вложенной зоны определяется всеми уровнями предшествующих зон, которые должен преодолеть злоумышленник, чтобы попасть во вложенную зону.

Виды контролируемых зон показаны на рисунке 1.3.

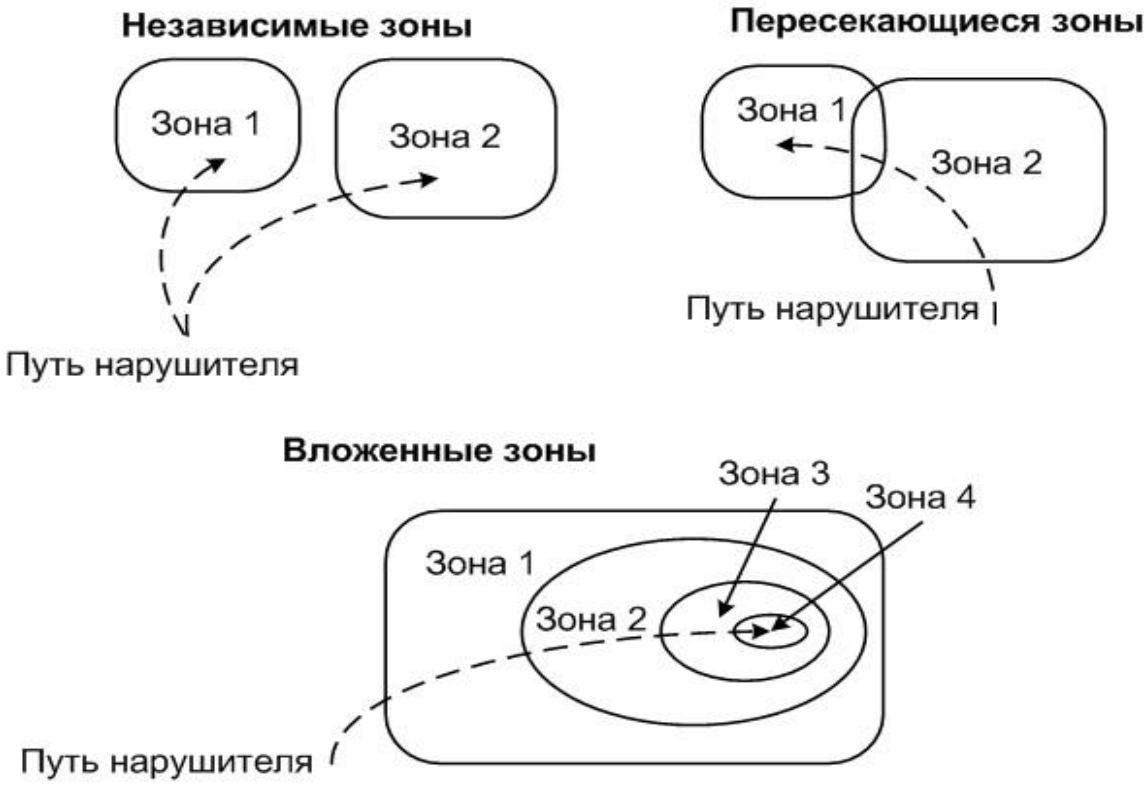


Рисунок 1.3 - Виды контролируемых зон

Каждая зона характеризуется уровнем безопасности находящейся в ней информации, или другими защищаемыми ресурсами. Безопасность информации в зоне зависит от количества рубежей защиты, эффективности применяемых средств и мероприятий защиты.

В зависимости от ценности защищаемых ресурсов, расположенных в контролируемых зонах, все зоны разделяются на категории. Чем выше ценность ресурсов (информации, материальных активов и др.), тем большее количество зон и рубежей защиты требуется организовать [25]. Классификация контролируемых зон по условиям доступа приведена в таблице 1.1.

Таблица 1.1 - Классификация контролируемых зон по условиям доступа

Категория	Наименование зоны	Функциональное назначение	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны	Технические средства охраны
I	Свободная	Места свободного посещения	Свободный	Свободный	Есть	Нет
II	Наблюдаемая	Комнаты приема посетителей	Свободный	Свободный	Есть	Средства наблюдения
III	Регистрационная	Кабинеты сотрудников	Свободный	Свободный с регистрацией по удостоверениям личности	Есть	Охранная сигнализация
IV	Режимная	Секретариат, компьютерные залы, архивы	По служебн. удостоверениям или идентификационным картам	По разовым пропускам	Усиленная охрана	Охранная сигнализация, система контроля доступа
V	Усиленной защиты	Кассовые операционные залы, материальные склады	По спецдокументам	По спецпропускам	Усиленная охрана	Охранная сигнализация (два рубежа), СКУД
VI	Высшей защиты	Кабинеты высших руководителей, зал для ведения переговоров, специальные хранилища	По спецдокументам	По спецпропускам	Усиленная охрана	Охранная сигнализация (два рубежа), СКУД, защита утечки информации, механическое усиление

I Свободная зона – помещения и прилегающая территория, доступ в которые свободен для любой категории лиц. За этими территориями не ведется наблюдения и там не размещено никаких технических средств охраны и безопасности. Примером такой зоны может быть бюро пропусков, справочное бюро и др.

II Наблюдаемая зона – помещения и территория, доступ в которые также не ограничен, но за ними ведется систематическое наблюдение силами службы безопасности или охраны. Наблюдение может вести лицо, находящееся в данном помещении или в других помещениях, с помощью оптических или телевизионных приборов. Типичным примером может служить вестибюль объекта, территория служебной автостоянки и др.

III Регистрационная зона – зона, вход в которую свободен для любого посетителя при условии, что он предъявит для регистрации документ, удостоверяющий его личность. Такая система часто используется в учреждениях, работающих с большим числом клиентов.

IV Режимная зона – зона, при входе в которую есть пост охраны. Проход допускается либо по пропускам установленной формы, либо по именным заявкам лиц, имеющих соответствующее право.

V Зона усиленной защиты – к этому типу зоны относятся помещения, в которые допускаются только сотрудники предприятия, а для посторонних лиц доступ туда возможен только по специальным пропускам или в сопровождении уполномоченных лиц. Такого рода помещения, как правило, оборудуются средствами контроля доступа и охранной сигнализацией. Вход в эту зону может также контролироваться постом охраны.

VI Зона высшей защиты – зона, вход в которую ограничен не только для клиентов и посетителей, но и для собственных сотрудников, не имеющих допуска в данные помещения. Примером могут служить помещения высшего руководства или помещения, связанные с хранением и обработкой особо ценной и конфиденциальной информации. Зона высшей защиты оборудуется

инженерно-техническими средствами защиты, приборами контроля и наблюдения и дополнительными постами охраны [4].

Представленные шесть категорий режимности помещений практически способны охватить все варианты функционального назначения служебных помещений. Отметим факторы, регламентирующие помещение по одной из вышеуказанных категорий:

– условия доступа сотрудников предприятия;

– условия доступа клиентов и посторонних лиц;

– наличие и вид физической охраны;

– виды использования технических средств наблюдения и охраны.

Кроме этого, нанесение на план здания защищаемого объекта, например, категорий режимности всех помещений, позволит наглядно увидеть все недостатки в распределении помещений по функциональному назначению. Наиболее оптимальным способом распределения помещений является компактное размещение в одном месте помещений одной и той же категории. При этом желательно, чтобы между собой соседствовали зоны одинаковых или не слишком различающихся категорий. Например, попасть в помещение IV зоны можно только из помещения III или V зоны. Это позволит наиболее экономным способом разместить средства инженерного усиления строительных конструкций и технические средства безопасности [6, 17].

На границах зон, а также на пути движения нарушителя создаются рубежи защиты. При этом важен принцип многорубежности физической защиты.

Многорубежность физической защиты – наличие на пути распространения источников угроз преград, уменьшающих энергию источников угроз и увеличивающих время продвижения нарушителя к цели.

Количество рубежей защиты и средства, используемые для их реализации, определяется ценностью защищаемых ресурсов. Пример построения многорубежной защиты приведен на рисунке 1.4.

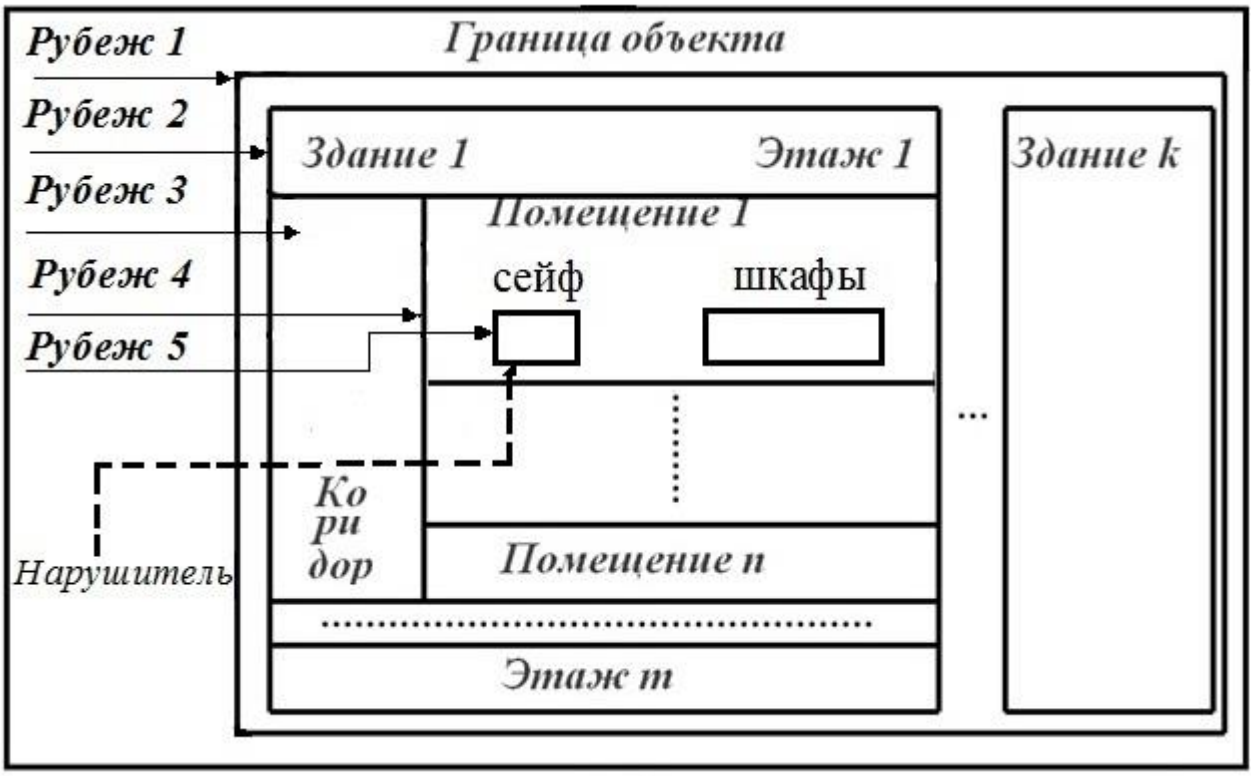


Рисунок 1.4 - Пример построения многорубежной защиты

На рисунке представлены следующие контролируемые зоны:

- территория;
- здание на территории;
- коридор;
- служебный кабинет;
- шкафы, сейф.

Соответственно рубежи защиты для данного примера:

- заграждение на границе объекта (рубеж 1);
- стены, двери, окна здания (рубеж 2);
- стены, двери, окна, потолок коридора (рубеж 3);
- стены, двери кабинета (рубеж 4);
- стены, двери шкафов, сейфов (рубеж 5).

Равнопрочность рубежа контролируемой зоны – это принцип эффективной защиты, заключающийся в том, по всему периметру рубежа реализована одинаково прочная защита (не имеет слабых мест).

Ограниченный доступ к элементам системы защиты – это необходимое условие для осуществления принципа скрытности защиты, доступ к элементам защиты должны иметь только сотрудники службы безопасности.

Адаптируемость системы защиты к новым угрозам достигается прогнозированием угроз и возможностью перенастройки средств защиты в соответствии с новыми угрозами без дополнительных капиталовложений.

Согласованность системы защиты с другими системами организации. Этот принцип необходим так как защитные мероприятия не должны препятствовать выполнению основных функций сотрудниками, не привносить в деятельность организации дополнительные трудности [7].

В качестве **способов защиты** выступают всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу.

1.3 Методы физической защиты объектов информатизации

Основной задачей физической защиты является предотвращение несанкционированного доступа нарушителя на объект защиты. Методы физической защиты должны обеспечивать задержку нарушителя на пути проникновения, обнаружение проникновения и нейтрализацию угроз безопасности [2].

Методы физической защиты объектов:

− создание физических, электронных и других препятствий злоумышленнику на пути к носителям конфиденциальной информации и ее источникам и другим защищаемым ресурсам;

− введение злоумышленника в заблуждение с помощью технических средств путем подготовки и распространения (навязывания) ложной информации;

− скрытие информации и ее носителей от злоумышленника на всех этапах добывания информации;

− применение различных средств контроля несанкционированного доступа для выявления попыток реализации злоумышленником угроз безопасности информации и информирование о выявленных попытках должностных лиц, участвующих в выработке мер защиты информации на объектах предприятия;

− предупреждение должностных лиц и персонала предприятия о возникновении чрезвычайных ситуаций на объектах.

Физическая защита обеспечивается организационными методами, методами инженерной защиты и технической охраны. Инженерная защита реализуется за счет естественных и искусственных преград на пути возможного нарушителя. Примером искусственных преград являются заборы, ворота, двери, стены, перекрытия, шкафы и т.п. Так как любые преграды могут быть преодолены, необходимо применять методы обнаружения вторжений в контролируемые зоны и их нейтрализацию. Такие методы называются технической охраной. Одним из них является скрытие информации.

Скрытие информации – группа методов защиты, которые основаны на создании условий и действий, затрудняющих поиск и обнаружение объектов защиты, распознавание и измерение их признаков, снятие с носителей. Скрытию подлежит как информация, так и ее носители. Скрытие бывает: пространственное, временное, структурное и энергетическое [17].

Пространственное скрытие предусматривает хранение информации или носителей в местах, заранее неизвестных возможному нарушителю. Перед нарушителем появляется задача поиска информации или ее носителя, что увеличивает время добывания информации. Временное скрытие предусматривает отсутствие у нарушителя данных о времени передачи интересующей его информации. Структурное сокрытие связано с созданием ложного информационного портрета сообщения, физического объекта или

сигнала. Энергетическое скрытие достигается созданием помех, затрудняющих перехват и распознавание информации нарушителем.

1.4 Нормативно-правовая база физической защиты

При построении системы физической защиты объекта информатизации необходимо руководствоваться нормативно-правовыми документами, утвержденными на уровне Постановлений Правительства РФ, Министерства внутренних дел РФ, МЧС РФ. Также важными документами являются строительный нормы и правила, которые предъявляют требования к строительным конструкциям зданий и сооружений для обеспечения их достаточной технической укрепленности и пожарной безопасности.

Нормативно-правовые документы МВД России предназначены для обеспечения защиты от преступных посягательств и антитеррористической защищенности зданий и сооружений. В этих документах описаны требования и рекомендации по выбору и установке систем тревожной сигнализации, средств охранно-пожарной сигнализации, средств технической укрепленности для оборудования объектов, систем контроля и управления доступом, систем пожарной безопасности, систем видеонаблюдения [13, 14,15,16].

Важное значение имеет определение категории защищаемого объекта, так как именно категория объекта определяет состав средств защиты, количество рубежей защиты и другие требования к системе безопасности объекта. Понятия «категория» и «защищенность» охраняемого объекта введены ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации» и будут рассмотрены в следующем разделе учебного пособия.

Список нормативно-правовых документов, которые необходимо применять при формировании состава и структуры СФЗ объекта приведены в таблице 1.2.

Таблица 1.2 - Нормативно-правовые документы физической защиты

Наименование документа	Область применения
1	2
РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств». Утвержден МВД РФ 6 ноября 2002 г.	Распространяется на вновь проектируемые, реконструируемые и технически перевооружаемые объекты различных форм собственности, охраняемые или подлежащие передаче под охрану подразделениям вневедомственной охраны при органах внутренних дел на территории РФ.
Свод правил СВ 132.13330.2011 «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования». Разработан Министерством регионального развития Российской Федерации, Федеральной службой безопасности Российской Федерации, МВД РФ.	Распространяется на проектирование зданий и сооружений и устанавливает минимально необходимые требования к проектным решениям, позволяющим обеспечить антитеррористическую защищенность объектов, направленным на: предотвращение несанкционированного доступа на объект производственного назначения физических лиц, транспортных средств и грузов; обнаружение взрывных устройств, оружия, боеприпасов.
Рекомендации Р 78.36.007-99 «Выбор и применение средств охранно- пожарной сигнализации и средств технической укрепленности для оборудования объектов». Утв. ГУВО МВД РФ 27 июня 1998 г.	Даны рекомендации и изложены требования, которые необходимо учитывать организациям, ведущим проектные и монтажные работы по оборудованию объектов ТС ОПС и средствами технической укрепленности.
ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации. Часть 1. Общие требования». Введен в действие постановлением Госстандарта РФ от 22 мая 1995 г. N 256	Устанавливает требования при проектировании, монтаже, наладке, испытаниях, эксплуатации и техническом обслуживании систем тревожной сигнализации, охранной, охранно-пожарной сигнализации, применяемых для обеспечения безопасности людей и имущества.

Продолжение таблицы 1.1

1	2
ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний». Разработан ФГУ НИЦ "ОХРАНА" МВД России, Центром оперативного руководства деятельностью вневедомственной охраны (ЦОРДВО) МВД России.	Распространяется на средства и системы контроля и управления доступом, предназначенные для предотвращения несанкционированного доступа людей, транспорта и других объектов в зону доступа (здания, помещения, территории, транспортные средства) в целях обеспечения противокриминальной защиты.
ГОСТ Р 51558- 2008 «Средства и системы охранные телевизионные». Разработан ФГУ НИЦ "ОХРАНА" МВД России, Центром оперативного руководства деятельностью вневедомственной охраны (ЦОРДВО) МВД России.	Распространяется на вновь разрабатываемые и модернизируемые охранные телевизионные средства и системы замкнутого типа, для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной защиты.
ГОСТ 53704-2009 «Системы безопасности комплексные интегрированные». Разработан ФГУ НИЦ "ОХРАНА" МВД России.	Предназначен для определения условий и ресурсов для объединения в сложную систему технических средств, применяемых для обеспечения безопасности защищаемых объектов с учетом их назначения и значимости от техногенных, антропогенных и природно-климатических угроз.
ГОСТ 12.1.004-91 ССБТ. «Пожарная безопасность. Общие требования». Разработан МВД СССР, Министерством химической промышленности СССР.	Устанавливает общие требования пожарной безопасности к объектам защиты различного назначения на всех стадиях их жизненного цикла.
ГОСТ Р 22.1.12-2005 «Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений». Разработан ФГУ ВНИИ по проблемам гражданской обороны и чрезвычайных ситуаций.	Настоящий стандарт устанавливает: - категории потенциально опасных объектов, зданий и сооружений (далее - объектов), подлежащих оснащению структурированными системами мониторинга и управления инженерными системами зданий; - основные требования к СМИС.

Продолжение таблицы 1.1

1	2
ГОСТ Р 50862-2012 «Сейфы, сейфовые комнаты и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому». Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2012 г. N 1031-ст.	В настоящем стандарте реализованы положения и нормы Федерального закона "О техническом регулировании", стандарта Европейского комитета по стандартизации (CEN) ЕН 1143-1:1997 «Хранилища ценностей. Требования, классификация и методы испытаний на устойчивость к взлому. Часть 1. Сейфы, двери кладовых и кладовые ценностей».
РД 25.952-90 «Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Порядок разработки задания на проектирование». Утвержден Министерством электротехнической промышленности и СССР.	Настоящий руководящий документ распространяется на проектирование автоматических систем пожаротушения, пожарной, охранной и охранно-пожарной сигнализации (далее - системы пожаротушения и сигнализации) для зданий и сооружений различного назначения.
Федеральным законом № 117-ФЗ от 10 июля 2012 г. «Технический регламент о требованиях пожарной безопасности».	Дана классификация зданий, сооружений и помещений по пожарной и взрывопожарной опасности для установления требований пожарной безопасности, направленных на предотвращение возможности возникновения пожара и обеспечение противопожарной защиты.
РД 78.148-94 «Защитное остекление Классификация, методы испытаний». Утвержден МВД СССР	Распространяется на защитное остекление, устанавливаемое на объектах различных видов собственности, охраняемых или подлежащих передаче под охрану вневедомственной охраны.
ГОСТ 26342-84 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры.	Распространяется на технические средства охранно-пожарной сигнализации для защиты объектов народного хозяйства, квартир и других мест хранения личного имущества от несанкционированного проникновения человека или пожара, и устанавливает типы, основные параметры и размеры этих средств.

2 Анализ объектов физической защиты

2.1 Схема анализа защищаемого объекта информатизации

Для осуществления выбора состава и средств физической защиты, эффективно обеспечивающих безопасность защищаемого объекта необходимо провести его тщательное обследование. Схема анализа защищаемого объекта представлена на рисунке 2.1.

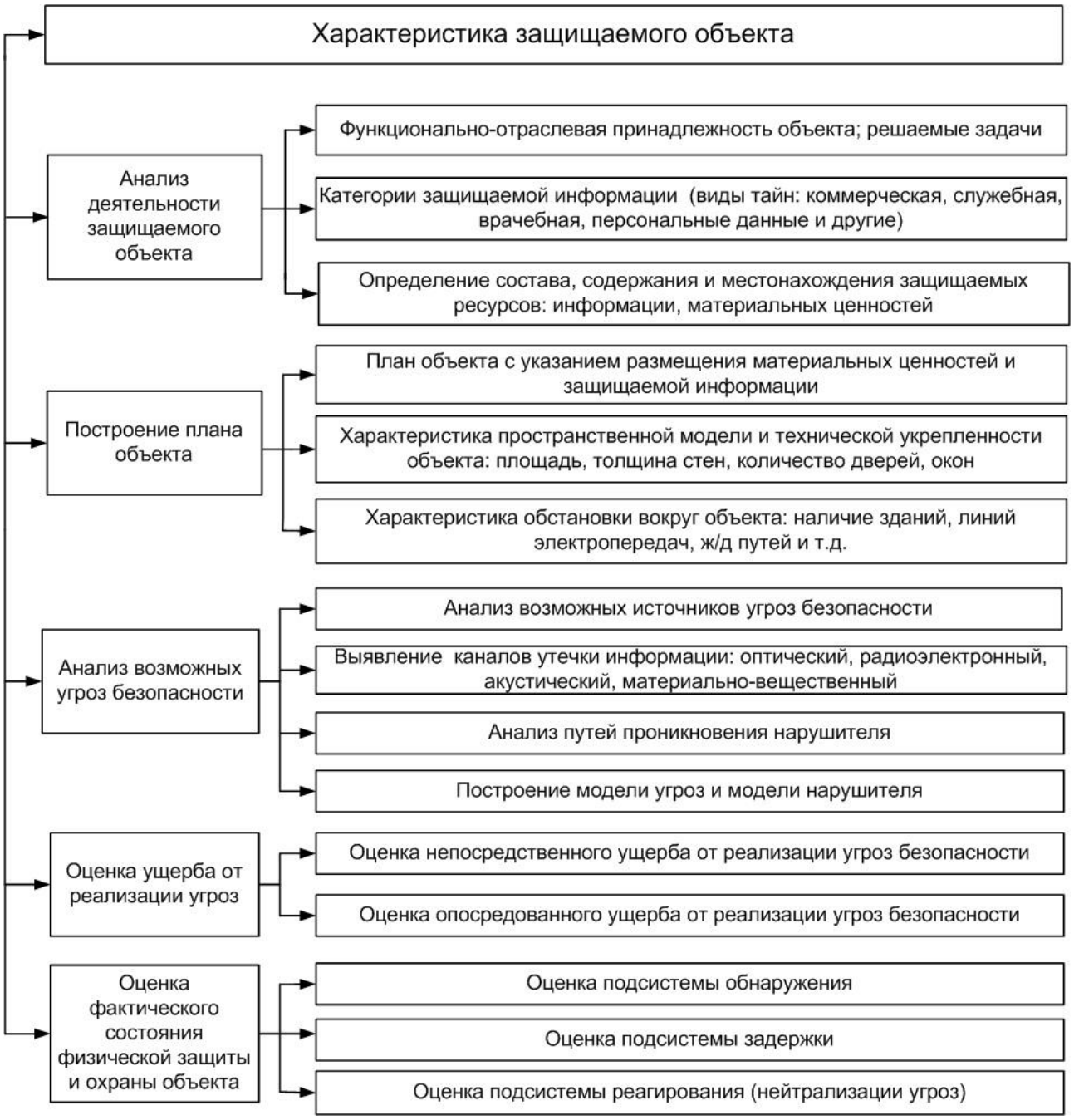


Рисунок 2.1 – Схема анализа защищаемого объекта

Анализ деятельности защищаемого объекта включает в себя определение его функционально-отраслевой принадлежности. С точки зрения защиты классификация объектов может быть проведена по нескольким признакам: по назначению, по степени пожаро- и взрывоопасности, по виду потерь, по масштабу потенциальных потерь, по объему производства, по количеству персонала и т.д. [20, 21, 27].

По назначению все объекты делятся на:

- производственные;
- строительные;
- транспортные;
- топливно-энергетического комплекса;
- оборонно-промышленного комплекса;
- социального назначения;
- культурного назначения.

Для характеристики потенциальной опасности объекта сформулированы пять видов и масштабов потерь:

- политические (определяются возможным подрывом авторитета власти, возникновением политической нестабильности);
- людские (выражаются в нанесении вреда жизни и здоровью людей);
- финансовые (определяются материальными потерями);
- экологические (нанесение вреда природным ресурсам);
- культурные (потери, свзанные с утратой художественных ценностей, памятников архитектуры и т.д.);

Масштабы потенциальных потерь:

- локальный (в пределах одного объекта);
- местный (в пределах населенного пункта);
- территориальный (в пределах территории субъекта России);
- региональный (затрагивающий масштабы региона);
- государственный (затрагивает более двух субъектов РФ);
- межгосударственный (выходит за пределы страны).

При анализе деятельности защищаемого объекта необходимо определить состав, содержание и местонахождение защищаемых ресурсов: информации, материальных ценностей, так как в зависимости от ценности этих ресурсов формируется вывод о видах и масштабах потенциального ущерба при реализации возможных угроз безопасности [5, 37].

К объектам (ресурсам), подлежащим защите от потенциальных угроз и противоправных посягательств, относятся:

− персонал компании (руководящие работники, производственный персонал, имеющий непосредственный доступ к финансам, валюте, ценностям, хранилищам, осведомленные в сведениях, составляющих коммерческую тайну, работники внешнеэкономических служб и другие);

− финансовые средства;

− информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;

− средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной, телефонной, факсимильной, радиосвязи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

− материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);

− технические средства и системы охраны и защиты материальных и информационных ресурсов.

Все объекты, в отношении которых могут быть осуществлены угрозы безопасности или противоправные посягательства, имеют различную потенциальную уязвимость с точки зрения возможного материального или

морального ущерба. Исходя из этого они должны быть проранжированы по уровням уязвимости (опасности), степени риска.

Наибольшую уязвимость представляют финансовые и информационные ресурсы и некоторые категории персонала.

Следующим обязательным пунктом анализа объекта защиты является построение плана его территории и помещений с указанием местонахождения защищаемых ценностей. На плане необходимо провести разделение объекта на контролируемые зоны, определить категорию зон в соответствии с таблицей 1.1. Строят пространственную модель объекта защиты с указанием количества дверей, окон, толщины стен, характеристикой близко расположенных зданий, линий электропередач и т.д.

Важным этапом является построение модели угроз безопасности, этот процесс включает в себя анализ источников угроз, анализ уязвимых мест объекта, построение модели нарушителя. На последнем этапе обследования объекта необходимо проанализировать применяемые средства и мероприятия по физической защите данного объекта, и сделать вывод о достаточности или недостаточности реализованной защиты [31].

Далее более подробно остановимся на категорировании объекта защиты, так как определение категории объекта определяет состав и выбор средств физической защиты.

2.2 Категорирование защищаемой информации

Категорированием защищаемой информации называют установление градации важности информации. Для информационных ресурсов существует классификация по уровню секретности или важности. Все виды информации можно сразу разделить на две группы: содержащие государственную тайну и не содержащие государственную тайну. Согласно Федеральному закону N 5485-1 «О государственной тайне», **государственная тайна** – это защищаемые государством сведения в области его военной, внешнеполитической,

экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. В статье 8 этого закона указаны степени секретности сведений и грифы секретности носителей этих сведений.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений. Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

– **особой важности**: к сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

– **совершенно секретные**: к совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

– **секретные:** к секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесённый интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации. Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

В Федеральном законе № 5485-1 указаны и сведения, не относящиеся к государственной тайне, а также порядок отнесения информации к государственной тайне.

Вся другая информация, не содержащая государственную тайну, но подлежащая защите, называется конфиденциальной. Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» введены определения данных сведений.

Конфиденциальной информацией называют документированную информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Конфиденциальная информация может быть личной, служебной, коммерческой, судебно-следственной, профессиональной, производственной.

К конфиденциальной личной информации относится информация, содержащая персональные данные, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке. Перечень сведений конфиденциального характера и краткое описание приведено в таблице 2.1.

Служебной тайной называют защищаемые сведения, не являющиеся государственной тайной, несанкционированное распространение которых служащим, которому эти сведения были доверены в связи с исполнением им должностных обязанностей, может нанести ущерб органам государственной власти, государственным предприятиям, учреждениям, организациям или нарушить их функционирование.

Таблица 2.1 - Категории конфиденциальной информации

Категория	Краткое описание
Персональные данные	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
Тайна следствия и судопроизводства	Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с ФЗ № 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" принято решение о применении мер государственной защиты, указанных лиц, если законодательством РФ такие сведения не отнесены государственной тайне.
Служебная тайна	Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.
Врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами.
Коммерческая тайна	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.
Сведения, составляющие интеллектуальную собственность	Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

К коммерческой тайне относятся сведения, содержащие действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим

лицам. К ней нет свободного доступа на законном основании, и обладатель информации принимает меры по охране ее конфиденциальности.

Судебно-следственная конфиденциальная информация содержит сведения, составляющие тайну следствия и судопроизводства.

К профессиональной конфиденциальной информации относится информация, содержащая сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебными, нотариальными, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений).

Производственная конфиденциальная информация содержит сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации. Информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных. [ФЗ №149 «Об информации, информационных технологиях и о защите информации»].

2.3 Категорирование объектов защиты по уровню важности

Для обеспечения корректности технических требований при проектировании систем физической защиты необходимо провести категорирование защищаемого объекта.

Понятие «категория охраняемого объекта» введено ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации». Категория охраняемого объекта - это комплексная оценка состояния объекта, учитывающая его экономическую или иную (например, культурную) значимость в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны.

Цель категорирования на современном этапе была сформулирована как «создание системы категорирования, предполагающей дифференциацию требований к системе антитеррористической и противокриминальной защиты объектов, обеспечивающей минимально необходимые и достаточные уровни безопасности объектов в соответствии с их категориями потенциальной опасности, с учетом критериев оценки возможного ущерба интересам личности, общества и государства, который может быть нанесен преступными действиями в случае невыполнения требований, предъявляемых к системе защиты объекта» [20, 22].

Критерии, которые должны быть учтены при категорировании объектов, проанализированы в источниках [8,27,28] включают такие важные характеристики, как потенциальная опасность, значимость объектов по функционально-отраслевым признакам, уровень секретности информации, вид и величина ущерба от аварий, численность персонала, материальные активы, наличие пожаро- и взрывоопасных веществ и другие. Классификация критериев категорирования объектов представлена на рисунке 2.2.

Качественные критерии подразумевают деление объектов на две группы.

- **объекты группы А:** особо важные, повышенной опасности и жизнеобеспечения, противоправные действия на которых могут привести к крупному ущербу государству, экологии или владельцу имущества;
- **объекты группы Б:** важные объекты, хищения на которых могут привести к ущербу в размере свыше 500 МРОТ.

Рисунок 2.2 – Классификация критериев категорирования объектов

Согласно руководящему документу РД 78.36.003-2002 **особо важный объект** - это объект, значимость которого определяется органами государственной власти Российской Федерации или местного самоуправления с целью определения мер по защите интересов государства, юридических и физических лиц от преступных посягательств и предотвращения ущерба, который может быть нанесен природе и обществу, а также от возникновения чрезвычайной ситуации.

Классификация объектов по уровню важности приведена в таблице 2.2.

Таблица 2.2 – Классификация объектов по уровню важности

Группа (категория)	Под-группа	Примеры объектов
1	2	3
Группа А – особо важные, повышенной опасности и жизнеобеспечения	А1	− объекты, включенные в Перечень объектов подлежащих государственной охране согласно постановления Правительства Российской Федерации г. N 587 (1992 г.); − объекты, включенные органами власти субъектов Российской Федерации или местного самоуправления в перечни объектов особо важных, повышенной опасности и жизнеобеспечения; − объекты по производству, хранению и реализации наркотических веществ, сильнодействующих ядов и химикатов, токсичных и психотропных веществ и препаратов (базы аптекоуправления, аптеки, склады медрезерва, научные, медицинские и другие учреждения, заведения, в практике которых используются эти вещества); − ювелирные магазины, базы, склады и другие объекты, использующие в своей деятельности ювелирные изделия, драгоценные металлы и камни; − объекты и помещения для хранения оружия и боеприпасов, радиоизотопных веществ и препаратов, предметов старины, искусства и культуры; − объекты кредитно-финансовой системы (банки, операционные кассы вне кассового узла, дополнительные офисы, пункты обмена валюты, банкоматы); − кассы предприятий, организаций, учреждений, головные кассы крупных торговых предприятий; − сейфовые комнаты, предназначенные для хранения денежных средств, ювелирных изделий, драгоценных металлов и камней; − другие аналогичные объекты и имущественные комплексы.
	А2	специальные помещения объектов особо важных и повышенной опасности: − хранилища и кладовые денежных и валютных средств, ценных бумаг; − хранилища ювелирных изделий, драгоценных металлов и камней; − хранилища секретной документации, изделий; − специальные хранилища взрывчатых, наркотических, ядовитых, бактериологических, токсичных и психотропных веществ и препаратов; − специальные фондохранилища музеев и библиотек.

Продолжение таблицы 2.2

1	2	3
Группа В - важные объекты	В1	− объекты с хранением или размещением изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и другого имущества; − объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски и другие аналогичные объекты).
	В2	− объекты с хранением или размещением товаров, предметов повседневного спроса, продуктов питания, компьютерной техники, оргтехники, видео- и аудиотехники, кино- и фотоаппаратуры, натуральных и искусственных мехов, кожи, автомобилей и запасных частей к ним, алкогольной продукции с содержанием этилового спирта свыше 13% объема готовой продукции и другого аналогичного имущества.

Объект жизнеобеспечения: совокупность жизненно важных материальных, финансовых средств и услуг, сгруппированных по функциональному предназначению и используемых для удовлетворения жизненно необходимых потребностей населения (например, в виде продуктов питания, жилья, предметов первой необходимости, а также в медицинском, санитарно-эпидемиологическом, информационном, транспортном, коммунально-бытовом обеспечении и другие).

Объект повышенной опасности: объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво-, пожароопасные, опасные химические и биологические вещества, создающие реальную угрозу возникновения источника чрезвычайной ситуации.

Охраняемый объект: предприятие, организация, жилище, их часть или комбинация, оборудованные действующей системой охраны и безопасности.

Объекты, не вошедшие в перечни, классифицируются по ближайшему аналогу с учетом возможного риска и ущерба вследствие преступного посягательства на них.

Каждой подгруппе объектов должен соответствовать определенный класс (степень) защиты конструктивных элементов (ограждающих конструкций и элементов инженерно-технической укрепленности). **Класс защиты** - комплексная оценка, учитывающая размещение, прочностные характеристики, особенности конструктивных элементов и показывающий степень достаточности обеспечения надлежащей защиты объекта, оборудованного системой охранной сигнализации.

Руководящий документ РД 78.36.003-2002 устанавливает требования к классам защиты применяемых физических средств в соответствии с категорией важности объекта.

2.4 Категорирование объектов защиты по пожарной и взрывопожарной опасности

Классификация зданий, сооружений и помещений по пожарной и взрывопожарной опасности проводится Федеральным законом № 117-ФЗ от 10 июля 2012 г. «Технический регламент о требованиях пожарной безопасности».

По пожарной и взрывопожарной опасности помещения производственного и складского назначения независимо от их функционального назначения подразделяются на следующие категории:

- повышенная взрывопожароопасность (А);
- взрывопожароопасность (Б);
- пожароопасность (В1 - В4);
- умеренная пожароопасность (Г);
- пониженная пожароопасность (Д).

Здания, сооружения и помещения иного назначения разделению на категории не подлежат. Категории помещений по пожарной и взрывопожарной опасности определяются исходя из вида находящихся в помещениях горючих веществ и материалов, их количества и пожароопасных свойств, а также исходя из объемно-планировочных решений помещений и характеристик проводимых

в них технологических процессов. Определение категорий помещений следует осуществлять путем последовательной проверки принадлежности помещения к категориям от наиболее опасной (А) к наименее опасной (Д). Категории помещений по взрывопожарной и пожарной опасности представлены в таблице 2.3.

Таблица 2.3 - Категории помещений по взрывопожарной опасности

Категория помещения	Характеристика веществ и материалов, находящихся (обращающихся) в помещении
А повышенная взрывопожаро-опасность	Горючие газы, легковоспламеняющиеся жидкости с температурой вспышки не более 28 °С в таком количестве, что могут образовывать взрывоопасные парогазовоздушные смеси, при воспламенении которых развивается расчетное избыточное давление взрыва в помещении, превышающее 5 кПа, и материалы, способные взрываться и гореть при взаимодействии с водой, кислородом воздуха или друг с другом, в таком количестве, что расчетное избыточное давление взрыва в помещении превышает 5 кПа
Б взрывопожаро-опасность	Горючие пыли или волокна, легковоспламеняющиеся жидкости с температурой вспышки более 28 °С, горючие жидкости в таком количестве, что могут образовывать взрывоопасные пылевоздушные или паровоздушные смеси, при воспламенении которых развивается расчетное избыточное давление взрыва, превышающее 5 кПа
В1-В4 пожаро-опасность	Горючие и трудногорючие жидкости, твердые горючие и трудногорючие вещества и материалы (в том числе пыли и волокна), вещества и материалы, способные при взаимодействии с водой, кислородом воздуха или друг с другом только гореть, при условии, что помещения, в которых они находятся (обращаются), не относятся к категории А или Б
Г умеренная пожароопас-ность	Негорючие вещества и материалы в горячем, раскаленном или расплавленном состоянии, процесс обработки которых сопровождается выделением лучистого тепла, искр и пламени, и горючие газы, жидкости и твердые вещества, которые сжигаются или утилизируются в качестве топлива
Д пониженная пожароопас-ность	Негорючие вещества и материалы в холодном состоянии

Требования к способам обеспечения пожарной безопасности системы противопожарной защиты определяет ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность. Общие требования. Данный документ устанавливает общие требования пожарной безопасности к объектам защиты различного назначения на всех стадиях их жизненного цикла. Пожарная безопасность объекта должна обеспечиваться системами предотвращения пожара и противопожарной защиты, в том числе организационно-техническими мероприятиями.

Системы пожарной безопасности должны характеризоваться уровнем обеспечения пожарной безопасности людей и материальных ценностей, а также экономическими критериями эффективности этих систем для материальных ценностей, с учетом всех стадий (научная разработка, проектирование, строительство, эксплуатация) жизненного цикла объектов и выполнять одну из следующих задач:

- исключать возникновение пожара;
- обеспечивать пожарную безопасность людей;
- обеспечивать пожарную безопасность материальных ценностей;
- обеспечивать пожарную безопасность людей и материальных ценностей одновременно.

Объекты должны иметь системы пожарной безопасности, направленные на предотвращение воздействия на людей опасных факторов пожара, в том числе их вторичных проявлений, на требуемом уровне [12].

Объекты, пожары на которых могут привести к массовому поражению людей, находящихся на этих объектах, и окружающей территории опасными и вредными производственными факторами (по ГОСТ 12.0.003), а также опасными факторами пожара и их вторичными проявлениями, должны иметь системы пожарной безопасности, обеспечивающие минимально возможную вероятность возникновения пожара. Конкретные значения минимально возможной вероятности возникновения пожара определяются проектировщиками и технологами при паспортизации этих объектов.

3 Модель угроз и модель нарушителя физической безопасности

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

Причинами возникновения угроз могут быть (фактор неопределенности):

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

Исходными данными для проведения оценки и анализа угроз безопасности 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;
- оценить возможные последствия реализации угроз.

3.1 Анализ возможных источников угроз безопасности

Физическая безопасность работает с набором угроз, уязвимостей и контрмер, отличающимся от компьютерной и информационной безопасности. Угрозы физической безопасности в большей степени направлены на кражу, вандализм, терроризм, а также могут быть связаны с природными катаклизмами и политическими событиями.

Угрозы направлены на защищаемые объекты:

- персонал;
- финансовые средства;
- информация, носители информации;
- средства и системы информатизации (автоматизированные системы и вычислительные сети, линии телеграфной, телефонной, факсимильной, радиосвязи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);
- материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);
- объекты, обеспечивающие жизнедеятельность предприятия (энерго, тепло, водоснабжение).
- технические средства и системы охраны и защиты ресурсов.

Важное место среди защищаемых объектов занимает информация и носители информации. Для анализа угроз безопасности информации необходимо рассматривать два вида угроз: угроза воздействия нарушителя на информацию (кража, искажение, разглашение, модификация и т.д.) и угроза утечки по различным каналам: акустическим, визуально-оптическим, электромагнитным, материально-вещественным.

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

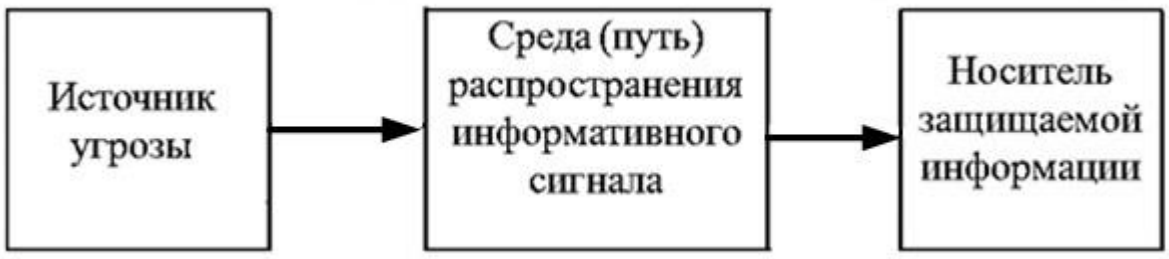


Рисунок 3.1 - Основные элементы угроз утечки информации

Угрозы утечки информации по техническим каналам:

− угрозы утечки речевой (акустической) информации по техническим каналам;

− угрозы утечки видовой (графической) информации ограниченного доступа визуальнооптическими средствами;

− 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.

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.

Все множество источников угроз физической безопасности можно разделить на антропогенные и естественные. Антропогенные источники угроз связаны с деятельностью человека, естественные источники угроз включают техногенные и стихийные источники угроз. Стихийные источники угроз включают обстоятельства, составляющие непреодолимую силу, носящие объективный и абсолютный характер. К стихийным источникам относятся:

– природные катаклизмы;

– события социально-политического характера.

Классификация угроз безопасности представлена на рисунке 3.2.

Рисунок 3.1 – Источники угроз физической безопасности

Техногенные источники угроз - это технические средства и технологии, которые могут выйти из-под контроля человека. К техногенным источникам угроз относятся:

- средства связи;
- сети электропитания;
- системы кондиционирования;
- технические средства обработки информации;
- программное обеспечение (ПО).

Техногенные источники угроз могут быть как внешними, так и внутренними. К внешним техногенным источникам угроз относятся:

− сбои в электроснабжении объекта;

− нарушения в работе систем жизнеобеспечения зданий;

− нарушения в работе вычислительных сетей из-за внешних воздействий;

− сбои в работе сетей телефонной связи.

К внутренним техногенным источникам угроз относятся:

− неправильное конфигурирование инженерно-технических средств защиты (систем СКУД, ОПС, видеонаблюдения и связи), приводящие к непроизводительным затратам;

− незапланированная потеря каналов связи, невозможность управления системой охранно-пожарной сигнализации и видеонаблюдения на объектах с пульта централизованного наблюдения;

− нарушение функционирования пульта централизованного наблюдения у оперативного дежурного (некомпетентность оператора, сбой программного обеспечения, выход из строя отдельных комплектующих компьютера, др.);

− нарушение работы системы СКУД, несанкционированный пропуск посторонних лиц на территорию объектов, допуск к материальным ценностям, конфиденциальной информации.

Антропогенные источники - субъекты внутри или вне организации, целенаправленные или ошибочные действия которых являются причиной нарушения безопасности . К ним относятся нарушители внешние и внутренние.

3.2 Модель нарушителя физической безопасности

Нарушитель - лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, пользователя, владельца, а также лицо, оказывающее ему содействие в этом.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов все нарушители могут быть отнесены к следующим двум категориям:

− категория I – лица, не имеющие права доступа в контролируемую зону;

− категория II – лица, имеющие право доступа в контролируемую зону.

Все потенциальные нарушители подразделяются на:

− внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны;

− внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ. В качестве внешнего нарушителями из числа лиц категории I могут выступать:

− бывшие сотрудники предприятий отрасли;

− представители конкурирующих организаций;

− представители преступных организаций;

− промышленная разведка;

− представители обслуживающих организаций (монтаж оборудования, ремонт элементов системы жизнеобеспечения зданий и т.п.).

Внешний нарушитель может осуществлять:

− несанкционированное проникновение в контролируемые зоны;

− совершение кражи защищаемых ценностей и информации;

− перехват видовой информации из-за пределов КЗ;

− перехват речевой информации из-за пределов КЗ;

− перехват информации, обрабатываемой техническими средствами за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;

− деструктивные воздействия через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;

− несанкционированный доступ к защищаемым объектам организации с использованием специальных технических средств;

− перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами;

– вывод из строя элементов системы физической защиты.

Внутренний нарушитель - нарушитель из числа лиц, имеющих право доступа без сопровождения в охраняемые зоны, является сотрудником организации.

Наибольшую опасность для инфромационной безопасности предприятия представляют его сотрудники, так как они имеют доступ в контролируемые зоны и к служебной информации и достаточную осведомленность. Внутренние нарушители могут быть разделены на преднамеренных и непреднамеренных.

Непреднамеренные:

− совершающие нарушения по неосторожности, из-за непрофессионализма,

− манипулируемые (не осознающие совершаемых нарушений).

Преднамеренные:

− выполняющие задания внешних заинтересованных лиц (конкурентов, промышленной разведки и т.п.),

− в целях саботажа.

Модель (образ) нарушителя представляет собой его комплексную характеристику, отражающую его возможное психологическое состояние, уровень физической и технической подготовленности, осведомленности, которая позволяет оценить степень его способности в практической реализации проникновения.

Характеристики нарушителя учитываются при определении требований 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;

– возможности нарушителя (навык, опыт, количество, оснащенность-техника, оружие, транспорт).

Для описания моделей нарушителей в качестве критериев классификации рассматриваются следующие критерии.

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;

− 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 различными способами маскировки.

8 Степень технической оснащенности вероятного нарушителя.

9 Способ проникновения вероятного нарушителя на объект.

На основе изложенных критериев выделяют четыре категории нарушителя:

− 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;

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

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

− 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.

Типовая модель нарушителя представлена в таблице 3.1.

Таблица 3.1 - Типовая модель нарушителя

Тип нарушителя	Категория	Подготовленность нарушителя								
		Психофизическая			Техническая			Осведомленность		
		В	С	Н	В	С	Н	В	С	Н
Внутренние	Сотрудники, имеющие санкционированный доступ к материальным ценностям		+			+		+		
	Сотрудники, имеющие доступ к финансовым ценностям		+			+		+		
	Сотрудники, имеющие доступ к служебной информации	+			+			+		
	Сотрудники, имеющие доступ к элементам системы защиты		+			+			+	
	Обслуживающий персонал (охрана, инженерно-технические службы)			+		+			+	
Внешние	Уполномоченный персонал разработчиков, который имеет право на техническое обслуживание	+			+			+		
	Уволенный сотрудник		+			+			+	
	Недобросовестные партнеры		+			+			+	
	Конкуренты		+				+		+	
	Посетители			+			+			+

Формализованная модель нарушителя представляет собой математическое описание его, которое обычно строится на основе теории графов и методов нечеткой логики, позволяющих делать выводы на основе неполных сведений об анализируемом объекте. Формализованная модель нарушителя может быть основана на многокритериальном ранжировании с применением рейтингового метода. Формализация нечеткой информации проводится на основе лингвистического подхода с переходом к единой количественной шкале, при этом строятся базы знаний для модели определения уровня опасности потенциального нарушителя. Уровень нарушителя может быть в диапазоне от 0 – абсолютно неопасный нарушитель, до 1 – очень опасный нарушитель. Который способен проникнуть на объект и при этом достигнуть поставленной цели почти со стопроцентной вероятностью [3,19].

3.3 Характеристика каналов утечки защищаемой информации

Понятие «утечка» относится к защищаемой информации. Утечка информации – это несанкционированный перенос информации от ее источника к нарушителю. Утечка информации осуществляется за счет ее разглашения, утери или кражи носителей информации, переноса ее с помощью полей. При утечке информации, из-за увеличения круга ее потребителей, цена информации уменьшается [33, 34].

Физическая среда несанкционированного распространения носителя защищаемой информации от ее источника к нарушителю образует канал утечки информации. Вид канала утечки зависит от вида носителя информации. Основными классификационными признаками технических каналов утечки информации является физическая природа носителя, по этому признаку все каналы утечки бывают:

- оптические;
- радиоэлектронные;
- акустические;

- вещественные.

Классификация каналов утечки информации представлена в таблице 3.2.

Таблица 3.2 - Классификация каналов утечки информации

Признак классификации	Наименование канала	Пример, краткое описание
По виду носителя	оптические	окна, двери, прозрачные межкомнатные перегородки
	радиоэлектронные	Телефоны, розетки, линия электропередач. ПЭВМ, система оповещения, ОПС
	акустические	окна, двери, батареи, водопровод, стены
	вещественные	документы на бумажных носителях, черновики, отходы производства
По структуре	простые	состоят из одного канала утечки
	составные	состоят из нескольких каналов одновременно
По способу организации	случайные	одноразовое добывание информации
	организованные	создаются злоумышленником для регулярного добывания информации
По времени функционирования	постоянные	утечка носит регулярный характер
	эпизодические	утечка носит кратковременный характер
По степени скрытия информации	открытые	передача информации в открытом виде
	технически закрытые	с использованием технических средств сокрытия канала утечки
	зашифрованные	с использованием шифрования информации

Технический канал утечки информации характеризуется показателями, которые позволяют оценить риск утечки:

- пропускная способность канала утечки;
- длина технического канала утечки;
- относительная информативность канала.

Все эти показатели зависят от параметров источника сигнала, среды распространения и приемника сигнала.

Источник сигнала характеризуется следующими показателями:

- мощность сигнала;
- диаграмма направленности излучения сигнала;
- параметрами спектра сигнала;
- динамическим диапазоном сигнала.

Среда распространения характеризуется:

- скоростью распространения носителя в среде;
- коэффициентом передачи или ослабления энергии сигнала;
- видом и мощностью помех.

Основными параметрами приемника являются:

- диапазон принимаемых частот;
- чувствительность;
- селективность;
- вид и уровень искажений.

Наибольшими потенциальными возможностями по добыванию семантической информации о видовых демаскирующих признаках обладает оптический канал, в котором информация добывается путем фото и видеосъемки.

Основным каналом получения сигнальных демаскирующих признаков является радиоэлектронный канал. В значительном меньшем объеме утечка информации возможна в акустическом и вещественном каналах. Комплексное добывание информации осуществляется злоумышленником по нескольким параллельным или последовательным каналам утечки.

3.4 Модель угроз физической безопасности защищаемого объекта

Угрозы физической безопасности объектов определяются типом источников угроз и направлением действия угроз. Соответственно угрозы могут быть антропогенного, техногенного или стихийного характера, направлены они могут быть как на материальные, финансовые ценности, так и на защищаемую информацию. Типы угроз: диверсия, терроризм, нарушение технологических процессов, хищение материальных ресурсов, информации. Основные угрозы физической безопасности приведены в таблице 3.3

Таблица 3.3 - Основные угрозы физической безопасности

Угроза	Тип источника угроз
1	2
Несанкционированное проникновение в КЗ	Антропогенный
Совершение диверсии в КЗ	Антропогенный
Совершение террористических актов	Антропогенный
Несанкционированные действия, приводящие к нарушению производственных технологических процессов	Антропогенный
Несанкционированный доступ к компьютерам	Антропогенный
Кража технических средств с хранящейся в них информацией	Антропогенный
Кража носителей информации	Антропогенный
Кража материальных и финансовых ценностей	Антропогенный
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств	Антропогенный
Прослушивание телефонных и радиопереговоров	Антропогенный
Внедрение «закладок»	Антропогенный
Воздействие на технические средства в целях нарушения их работоспособности	Техногенный
Воздействие на программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации	Техногенный
Воздействие на средства защиты информации	Техногенный

Продолжение таблицы 3.3

1	2
Побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации	Техногенный
Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ	Техногенный
Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств	Техногенный
Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом	Техногенный
Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	Техногенный
Угроза пожара	Стихийный
Угроза наводнения	Стихийный
Отказы и сбои в работе инженерно-технических средств охраны	Техногенный
Отказы и сбои в работе системы электроснабжения	Техногенный
Незапланированная потеря каналов связи, невозможность управления системой ОПС и видеонаблюдения на объектах с пульта централизованного наблюдения	Техногенный
выход из строя системы видеонаблюдения	Техногенный
выход из строя СКУД	Техногенный
Непреднамеренные (ошибочные, случайные, без корыстных целей) нарушения установленных требований при работе с материальными ценностями, финансовыми ресурсами, информацией, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный
Преднамеренные (в корыстных целях, по принуждению, со злым умыслом, т.п.) действия сотрудников, допущенных к материальным, финансовым и информационным ресурсам, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный

Оценка угроз безопасности в результате несанкционированного проникновения злоумышленника на объект или в результате утечки информации по техническим каналам проводится с учётом вероятности реализуемости рассматриваемого пути или канала, а также с учётом цены соответствующего элемента информации.

Обеспечение эффективной безопасности предполагает решение проблем моделирования угроз, их количественной и качественной оценки с учетом сложности структурно-функционального построения системы безопасности, ее элементов, и данных о внешних воздействиях естественного и искусственного происхождения [30].

Модель угроз безопасности - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

Для построения модели угроз безопасности можно применить руководящие документы ФСТЭК, разработанные для защиты персональных данных. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной организации в складывающихся условиях обстановки. Частота реализации угроз безопасности определяется экспертным методом в соответствии с и на основании результатов обследования объекта.

Оценка вероятности реализации угрозы (Y2) определяется по четырем вербальным градациям:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (0);

− низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (2);

− средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны (5);

− высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты (10).

С учетом изложенного коэффициент реализуемости угрозы **Y** будет определяться соотношением

$$Y = (Y_1 + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

− если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;

− если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы средняя;

− если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы высокая;

− если $Y > 0{,}8$, то возможность реализации угрозы очень высокая.

Определение опасности угроз проводится экспертным методом с учетом результатов обследования объекта. Y1=5 для среднего уровня исходной защищенности.

Показателем опасности, имеет три значения:

− низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям;

− средняя опасность - если реализация угрозы может привести к негативным последствиям;

− высокая опасность - если реализация угрозы может привести к значительным негативным последствиям.

Определение актуальных угроз безопасности.

Актуальная угроза - угроза, которая может быть реализована и представляет опасность. Правила определения актуальности УБСКХ приведены в таблице 3.4.

Таблица 3.4 - Правила определения актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Пример модели угроз безопасности защищаемого объекта приведен в таблице 3.5

Таблица 3.5 - Модель угроз безопасности защищаемого объекта

Угроза	Вероят-ность реализаци и угрозы	Возмож-ность реализации угрозы	Показатель опасности угрозы	Актуаль-ность угрозы
Несанкционированный доступ к компьютерам	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная
Кража технических средств с хранящейся в них информацией	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуаль-ная
Кража носителей информации	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуальн ая
Кража материальных и финансовых ценностей	Средняя вероят-ность (5)	0,5 (средняя)	Высокая	Актуальная
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероят-ность (5)	0, 6 (средняя)	Высокая	Актуальная

Особое внимание исследований [10, 11] уделено выбору математических методов исследования моделей угроз. При построении модели подчеркивается необходимость учитывать, что угрозы безопасности носят вероятностный характер и имеют высокую степень априорной неопределенности. При оценке угроз безопасности предлагаются:

− теория надежности для описания угроз, создаваемых техническими средствами (сбои, отказы, ошибки и т.д.);

− математическая статистика для описания естественных угроз (природные явления, стихийные бедствия и т.д.);

− теория вероятности для описания угроз, создаваемых людьми по небрежности, халатности и т.д.);

− экспертные методы для описания умышленных угроз.

Рассматривая основное назначение интегрированной системы безопасности как борьбу с угрозами различного характера, авторы считают возможным в качестве одного из комплексных критериев оценки эффективности системы безопасности использовать количественный показатель, связанный с числом угроз, защиту от которых она может обеспечить.

Появление угроз нового характера (экономических, информационных, юридических и других) требует включения в систему безопасности дополнительных средств и подсистем для защиты от данного вида угроз.

4 Физические средства подсистемы задержки

Подсистема задержки предназначена для обеспечения задержки (замедления) проникновения нарушителя в контролируемую зону, создание препятствий его несанкционированным действиям.

Средства задержки объединяют конструкции, затрудняющие движение злоумышленника и распространение стихийной силы к источнику информации, или материальным ценностям, и включают ограждения территории, зданий, помещений, шкафы, сейфы, хранилища, а также системы контроля и управления доступом людей, транспорта в контролируемые зоны.

4.1 Физические барьеры

К средствам задержки относятся физические барьеры. **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:

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

− предотвращение (усложнение) наблюдения за охраняемым объектом.

В состав физических барьеров входят :

− основное заграждение,

− предупредительное заграждение,

− заградительные инженерные средства,

− ворота, калитки, шлюзы.

Совместные задачи физических барьеров это 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.

Классификация физических барьеров приведена на рисунке 4.1.

Рисунок 4.1 - Классификация физических барьеров

4.2 Виды защитных ограждений

Ограждения по назначению делятся на основные, дополнительные, предупредительные. Основным ограждением территории является забор, ограда. Дополнительное ограждение предназначено для повышения

укрепленности основного ограждения. На предупредительном ограждении устанавливаются таблички «Запретная зона», «Не подходить» и т.д.

Главная функция основного заграждения - это препятствовать физически свободному проходу на территорию охраняемого объекта посторонних лиц и животных. Это своего рода декларированная собственником граница, пересечение которой для посторонних лиц противозаконно и позволяет собственнику применять к нарушителю разрешенные законом меры.

Основное заграждение, как и любое инженерно-строительное сооружение, характеризуется обликом, материалом и конструкциями изготовления, получаемыми при конкретном варианте исполнения, и, соответственно, имеет большое разнообразие вариантов технической реализации. Классификация основного ограждения приведена на рисунке 4.2.

Рисунок 4.2 - Классификация основного ограждения

Ограждения по степени защиты делят на 4 класса в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств». Выбор конструкций и материалов основного ограждения объекта, обеспечивающих требуемую надежность защиты объекта, производится в соответствии с этим руководящим документом в зависимости от категории защищаемого объекта.

1 Ограждения 1 класса защиты (минимально необходимая степень защиты объекта от проникновения) - ограждения из различных некапитальных конструкций высотой не менее 2 м. Для объектов категории БI.

2 Ограждения 2 класса защиты (средняя степень защиты объекта от проникновения) - ограждения деревянные сплошные (толщина доски не менее 40 мм) металлические сетчатые или решетчатые высотой не менее 2 м. Для объектов категории БII.

3 Ограждения 3 класса защиты (высокая степень защиты объекта от проникновения) - ограждения железобетонные, каменные, кирпичные, сплошные металлические высотой не менее 2,5 м. Для объектов категории АII.

4 Ограждения 4 класса защиты (специальная степень защиты объекта от проникновения) - ограждения монолитные железобетонные, каменные, кирпичные высотой не менее 2,5 м, оборудованные дополнительным ограждением. Для объектов категории АI.

В руководящем документе РД 78.36.003-2002 приведены подробные рекомендации по выбору вида ограждений для каждого типа объекта.

4.3 Ворота, калитки, двери

Ворота, калитки, двери – это традиционные инженерные конструкции для пропуска людей и транспорта на территорию или в помещения организации. Ворота устанавливаются на автомобильных и железнодорожных

въездах на территорию объекта. По периметру территории охраняемого объекта могут устанавливаться как основные, так и запасные или аварийные ворота.

Запирающие и блокирующие устройства при закрытом состоянии ворот должны обеспечивать соответствующую устойчивость к разрушающим воздействиям и сохранять работоспособность при повышенной влажности в широком диапазоне температур окружающего воздуха (минус 40 до +50 °С), прямом воздействии воды, снега, града, песка и других факторов. Замки на воротах должны быть гаражного типа или навесные.

Калитку следует запирать на врезной, накладной замок или на засов с висячим замком. Усиление защиты калиток рекомендуется выполнять аналогично способам усиления дверей и их коробок приведенным в приложении N 5.

Взломоустойчивость ворот характеризуется четырьмя степенями защиты, описанными в РД 78.36.003-2002. Ворота 1 степени защиты выполняются из некапитальных материалов высотой 1,5 м. Ворота 2 степени защиты высотой не менее 2 м, толщиной не менее 40 мм. Комбинированные и силовые ворота высотой не менее 2,5 м – 3 степень защиты. Металлические ворота не менее 2.5 м имеют 4 степень защиты.

Прочность дверей характеризуется устойчивостью к взлому, пулестойкостью, устойчивостью к взрыву. Различают двери с нормальной, повышенной и высокой устойчивостью.

Входные наружные двери на объект, по возможности, должны открываться наружу. Их следует оборудовать не менее двумя врезными (накладными) замками, установленными на расстоянии не менее 300 мм друг от друга или одним врезным (накладным) и одним висячим замками.

При применении сертифицированных дверей количество и класс замков указывается в соответствующей документации на дверь. Дверные проемы входов в специальные помещения объектов подгрупп AI и БII, в которых хранятся ценности (объекты подгруппы All, сейфовые и оружейные комнаты,

кассы предприятия и другие аналогичные помещения, требующие повышенных мер защиты) должны быть оборудованы дополнительной запирающейся металлической решетчатой дверью. Дополнительная дверь обеспечивает как защиту от скоротечной кражи, так и защиту персонала в помещении при работе с открытой входной дверью. Класс защиты дополнительной двери должен быть не ниже 2-го.

Надежность дверей и ворот определяется не только их механической прочностью, но и надежностью замков. По способу открытия замки делятся на механические и электроуправляемые. Механические замки открываются механическим ключом, для них характерно наличие ригеля, свальд, ключа, корпуса и запорной планки.

Типы электронных замков по методу запирания:

- соленоидный;
- электромагнитный;
- электромеханический.

Соленоидный электронный замок работает по типу соленоидного клапана, то есть при подаче напряжения на специальную катушку, образуется усилие, которое втягивает запирающую часть (замок закрыт), если напряжение отключается, запирающая часть отходит и освобождает дверь. Электромагнитный замок — самый распространенный тип, на его основе работают домофоны. Принцип работы заключается в том, что при подаче напряжения на электромагнит, возникает очень большая сила. Оторвать электромагнит практически нереально. Однако, если снять напряжение, дверь откроется сама. Электромеханический тип — запирающая часть приводится в движение специальным электромотором. То есть даже в случае отключения электричества, дверь будет закрыта.

В электронных замках установка кода, его хранение и сравнение с набранными цифрами производится с помощью микропроцессора. Виды электронных замков:

− электронный замок-невидимка;

− кодовый замок;

− биометрический замок;

− электронный замок с картой;

− комбинированная система.

Зарекомендовали себя с наилучшей стороны электронные замки с картой и биометрические замки. Распространение получили биометрические замки, использующие отпечаток пальца руки человека. Надежность такого замка достаточно высокая, характеризуется следующими показателями:

− FRR – вероятность ошибочного отказа сотруднику или количество ошибок данного рода (False Reject Rate) = 1 %;

− FAR – вероятность ошибочного пропуска нарушителя или количество ошибок данного рода (False Acceptance Rate) = 0,001 %;

4.4 Средства защиты окон

Окна в помещениях являются уязвимым звеном конструкции, так как предоставляют следующие угрозы:

− угроза проникновения нарушителя в контролируемую зону и совершение деструктивных действий;

− угроза наблюдения за контролируемой зоной;

− угроза перехвата видовой информации.

Особенно высокую опасность представляют окна первого этажа зданий. Требования по защите окон содержат в себе требования к прочности стекол, закрепления стекла в раме, установки решеток на окнах. Устанавливают защитное остекление с использованием закаленных, армированных, многослойных стеклопакетов.

В соответствии с РД 78.36.003-2002 «Техническая укрепленность» при оборудовании оконных конструкций металлическими решетками, их следует

устанавливать с внутренней стороны помещения или между рамами. В отдельных случаях допускается, по согласованию с подразделением вневедомственной охраны, установка решеток с наружной стороны при их обязательной защите техническими средствами охраны.

Если все оконные проемы помещения оборудуются решетками, одна из них делается открывающейся (распашной, раздвижной). Решетка должна запираться с внутренней стороны помещения на замок соответствующего класса защиты или на иное устройство, обеспечивающее надежное запирание решетки и эвакуацию людей из помещения в экстремальных ситуациях.

Для больших помещений с количеством окон более 5, количество открывающихся решеток определяется условиями быстрой эвакуации людей.

Оконные проемы первых этажей объектов (дач, коттеджей, садовых домиков и других строений) с длительным (сезонным) отсутствием собственников следует защищать щитами, ставнями не ниже 2-го класса защиты. При установки щитов и ставень с внешней стороны окна, они должны запираться на засов и висячий замок. При высоте окна более 1,5 м щиты и ставни должны запираться на два засова и два замка. Если защита осуществляется с внутренней стороны окна, щиты и ставни запираются только на засовы. Допускается для защиты оконных проемов использовать рольставни, жалюзи, решетки, которые по прочности и по возможности проникновения через них не уступают щитам и ставням.

Все оконные конструкции делятся на 4 класса защиты для объектов разных категорий.

Оконные конструкции 1 класса защиты (минимально необходимая степень защиты объекта от проникновения) - окна с обычным стеклом (стекло марки М4-М8 по ГОСТ 111-90, толщиной от 2,5 до 8 мм).

Оконные конструкции 2 класса (средняя степень защиты объекта от проникновения) - окна специальной конструкции с защитным остеклением класса А2 и выше по ГОСТ Р 51136-98, оборудованные деревянными ставнями

со сплошным заполнением полотен при их толщине не менее 40 мм, металлическими решетками произвольной конструкции.

Оконные конструкции 3 класса защиты (высокая степень защиты объекта от проникновения) - окна специальной конструкции с защитным остеклением класса А3 и выше по ГОСТ Р 51136-9, со щитами или деревянными ставнями со сплошным заполнением полотен при их толщине не менее 40 мм, обитыми с двух сторон стальными листами толщиной не менее 0,6 мм, металлическими решетками, изготовленными из стальных прутьев диаметром не менее 16 мм, образующих ячейки не более 150х150 мм или другими конструкциями соответствующей прочности.

Оконные конструкции 4 класса защиты (специальная степень защиты объекта от проникновения окна специальной конструкции с защитным остеклением класса БI и выше по ГОСТ Р 51136-98, окна с пулестойким стеклом (бронестекло) по ГОСТ Р 51136-98 класса 1 и выше.

В качестве косвенных защитных мероприятий выступают такие требования, как отсутствие наружных аварийных лестниц возле окон, отсутствие деревьев возле окон.

4.5 Шкафы, сейфы, хранилища

Шкафы, предназначенные для хранения конфиденциальных документов, ценных вещей, небольших сумм денег изготавливают из металла. При этом надежность шкафа определяется прочностью металла и устойчивостью замка к взлому. Для хранения особо ценных документов, вещей и денежных средств применяются сейфы и хранилища.

К сейфам относятся двустенные металлические шкафы с тяжелыми наполнителями пространства между стенками, в качестве которых используются армированные бетонные составы, многослойные заполнители из различных материалов. Сейфы и хранилища ценностей выбираются согласно

ГОСТ Р 50862-96 «Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость».

Хранилища представляют собой сооружение с площадью основания внутреннего пространства более 2 $м^2$, защищенное от взлома и устойчивое к воздействию высокой температуры при пожаре. По конструктивному исполнению хранилища подразделяются на:

- монолитные;
- сборные;
- сборно-монолитные.

Монолитные железобетонные хранилища размещают в подвалах здания на его фундаменте.

В соответствии с ГОСТ Р-50862-96 стойкость хранилищ и сейфов измеряется в условных единицах сопротивления, которые зависят от времени взлома с учетом коэффициента мощности применяемого инструмента. Интервал единиц стойкости разделен на 13 классов устойчивости к взлому. Группа самой высокой устойчивости составляют хранилища 11-13 классов. Время взлома их должно быть не менее 45-120 минут.

Сейфы имеют меньшую взломоустойчивость, чем хранилища. Сейфы с высокой устойчивостью относят к 7-10 классам. Взломоустойчивость сейфа зависит от стойкости замка. Чаще всего используют сувальдные ключевые замки, которые лучше цилиндровых защищены от взлома. Однако они нуждаются в высокой точности установки диска на соответствующее деление.

Сейфы оцениваются по пожаро- и влагоустойчивости. Устойчивость сейфа к температуре характеризуется временем, в течение которого температура внутри сейфа не превысит температуру возгорания бумаги.

Сейфы высокого класса имеют большой вес, который надо учитывать при выборе места их установки. При выборе сейфов следует учитывать: объем и тип вложения; вид предполагаемого воздействия; количество и типы замков, массогабаритные показатели; сумма страхового покрытия в случае взлома, которая изменяется в значительных пределах в зависимости от класса сейфа.

5 Средства подсистемы обнаружения нарушителей и пожара

Подсистема обнаружения нарушителя является центральным звеном системы физической защиты объекта, так как быстрота и надежность обнаружения вторжения определяет эффективность нейтрализации угроз. Подсистема обнаружения включает в себя: периметральные средства обнаружения, тревожную сигнализацию, систему видеонаблюдения, контрольно-пропускные пункты, систему контроля доступом.

5.1 Периметральные средства обнаружения

Периметр — внешняя граница (контур) защищаемой территории объекта, несанкционированное преодоление которого должно вызывать сигнал тревоги с указанием места его преодоления. Для эффективного решения задачи важно оптимальное сочетание механических преград, прежде всего пассивного ограждения (забора) периметра, с техническими средствами обнаружения (сигнализацией) [35].

Главная задача любой системы охраны периметра — обеспечение максимальной вероятности обнаружения нарушителя с точным указанием места проникновения для организации эффективного противодействия. В зависимости от особенностей объекта (его назначения, конструкции и конфигурации ограждения, климатических, геологических факторов и т.п.) линия периметра может быть оснащена как одним, так и несколькими рубежами охраны, либо целиком, либо на отдельных особо важных участках.

Однорубежная система охраны, в свою очередь, может быть создана на базе одного, наиболее подходящего для данных условий средства обнаружения, или же состоять из комбинации извещателей различного принципа действия. Например, нижняя и средняя части сетчатого ограждения защищаются кабельным чувствительным элементом, а козырек — лучевыми извещателями.

Многорубежная система охраны периметра с двумя и более рубежами, расположенными на расстоянии друг от друга, дает возможность определять направление движения нарушителя и позволяет сохранить работоспособность системы при выходе из строя одного из средств обнаружения.

В России природные условия отличаются большим разнообразием. Большие сезонные колебания температуры, в некоторых районах доходящие от 80° С до 90° С, сильные снегопады, метели, мокрый снег, гололед, иней, туманы, ураганные ветры, сильные дожди вызывают большие трудности при выборе соответствующего оборудования для защиты периметра.

При оснащении периметра средствами защиты необходимо учитывать факторы, влияющие на построение системы защиты:

- наличие полосы отчуждения;
- особенности рельефа местности;
- наличие вблизи объекта ж/д;
- наличие вблизи объекта линий электропередачи;
- виды растительности;
- трубопровод;
- разрыв периметра для проезда транспорта, прохода людей.

Виды растительности: Н - низкая (кустарник), С – средняя (высокие кусты акации, сирени и т.д.), В – высокая (деревья).

При необходимости вдоль основного ограждения периметра между основным и внутренним предупредительным ограждениями устраивают зону отторжения, в которой размещают:

— средства охранной и тревожной сигнализации;

— охранное освещение;

— средства охранного телевидения;

— посты охраны (постовые "грибки", наблюдательные вышки);

— средства связи постов и нарядов охраны;

— указательные и предупредительные знаки.

Для здания первым рубежом охраны должны быть защищены:

— оконные и дверные проемы по периметру здания или объекта;

— места ввода коммуникаций, вентиляционные каналы;

— выходы к пожарным лестницам;

Вторым рубежом охраны должен быть защищен объем помещения с помощью пассивных оптико-электронных извещателей с объемной зоной обнаружения, ультразвуковыми, радиоволновыми или комбинированными извещателями.

Третьим рубежом охраны должны быть защищены сейфы и отдельные предметы или подходы к ним с помощью емкостных, вибрационных, пассивных и активных оптико-электронных или радиоволновых извещателей.

Охрана периметра - это совокупность программных, технических, организационных средств и мероприятий, направленных на недопущение несанкционированного проникновения в охраняемый периметр.

Общие требования к периметральным системам:

− возможность раннего обнаружения нарушителя — еще до его проникновения на объект;

− точное следование контурам периметра, отсутствие “мертвых” зон;

− по возможности скрытая установка извещателей системы;

− независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т.д.);

− невосприимчивость к внешним факторам «нетревожного» характера — индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы;

− устойчивость к электромагнитным помехам — грозовые разряды, источники мощных электромагнитных излучений и т.п.

Все охранные извещатели классифицируются по следующим признакам:

− по типу обнаруживаемых тревожных событий;

− по виду контролируемой зоны;

− по способу приведения в действие;

− по принципу формирования информационного сигнала;

− по принципу действия.

На рисунке 5.1 приведена классификация охранных извещателей.

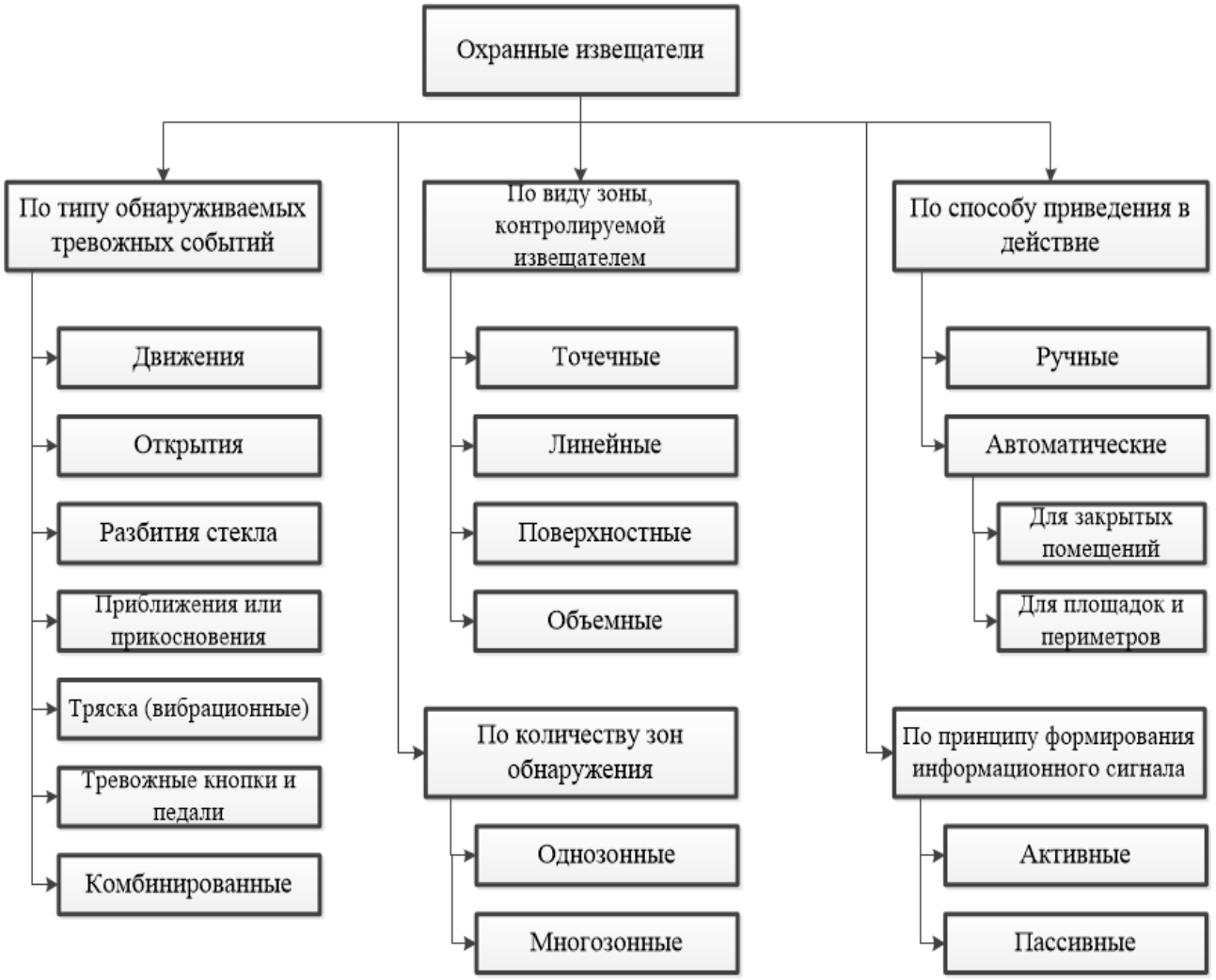


Рисунок 5.1 - Классификация охранных извещателей

Работа периметральной средств обнаружения 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.

Классификация периметральных средств обнаружения по принципу действия представлена на рисунке 5.2

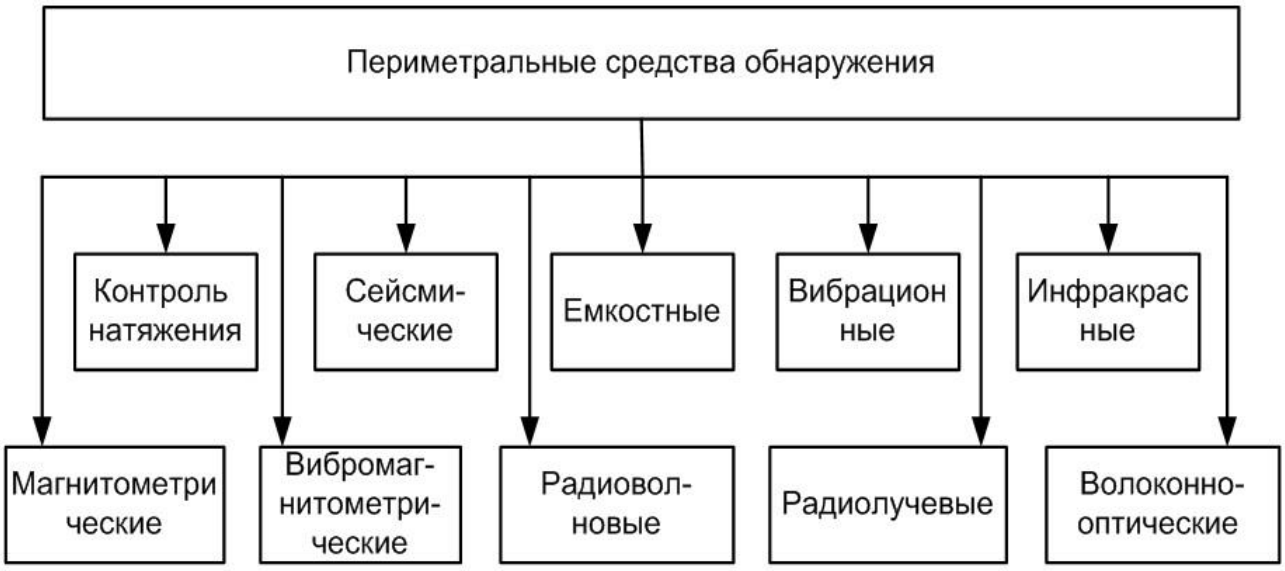


Рисунок 5.2 - Классификация периметральных средств обнаружения

Электромеханическое средство обнаружения, чувствительный элемент представляет собой натянутые нити из проволоки, на концах которых находятся датчики, малейшее изменение в размере нити, обрыв и перекусывание приведет к тревожному сигналу. Предназначено для блокирования объектов кратковременного базирования. Может применяться в качестве индивидуального средства охраны. Примером служит электромеханическое средство «Трос». Состав комплекта:

- блок П12БМ с автономным электропитанием;
- специальный микропровод, размещённый в сменной кассете.

Микропровод прокладывают на охраняемом рубеже. Блок П12БМ осуществляет контроль целостности этого провода и при его обрыве выдаёт звуковой сигнал. Проверка работоспособности указанного блока осуществляется автоматически при каждом его включении.

Сменная кассета обеспечивает удобство развёртывания средства обнаружения (СО) на местности одним человеком.

Возможно многократное использование данной кассеты до полного расхода микропровода. Развёрнутый микропровод повторно не используется. При необходимости вместо специального микропровода может применяться

любой тонкий изолированный медный провод, например, ПЭВ-2 диаметром 0,1 - 0,2мм. СО «Трос» хорошо маскируется и не требует для размещения предварительной инженерной подготовки местности. Влияние на работу СО других типов не оказывает, максимальная длинна охраняемого рубежа 1500 – 2000 м.

Вибрационное средство обнаружения, чувствительный элемент представляет собой 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).

Вибрационные и оптоволоконные средства обнаружения подлежат укладке в грунт, но при этом следует обеспечить возможность деформации чувствительного элемента. Как правило, извещатель, укладываемый в грунт, состоит из блока обработки сигналов и чувствительного элемента. Кабель может быть натянут на эластичную сетку или уже выпускаться производителем в виде сетки. Эта конструкция укладывается на мягкие маты, сверху посыпается гравием, галькой. Такой вариант установки вибрационного (и оптоволоконного) СО требует аккуратного использования в условиях суровой российской зимы, когда выпадает немало снега, а грунт промерзает.

Примером такого СО служит «Диамант». Вибрационное средство обнаружения (СО) «Диамант» предназначено для создания сигнализационных рубежей охраны периметров объектов. Использование всего комплекта составных частей позволяет на основе средства обнаружения «Диамант» строить замкнутые рубежи охраны периметров объектов. Высокие защитные свойства покрытия и эстетичный внешний вид линейной части, технологичность монтажа, позволяют использовать средство обнаружения «Диамант» для оснащения таких объектов как: стадионы и спортивные комплексы, аэропорты, административные учреждения и пр. СО обладает высокой сигнализационной надежностью: вероятность обнаружения – не менее 0,95 (при обнаружении нарушителя на ранней стадии до его проникновения на

объект); наработка на ложное срабатывание – не менее 2000 часов; наработка на отказ – не менее 30000 часов. Обеспечивается функционирование в условиях сложной помеховой обстановки, обусловленной воздействием как природно-климатических, так и промышленных помеховых факторов

Емкостное средство обнаружения, в котором изменяется емкость чувствительного элемента при проделывании отверстия, перелезании через преграду, что приводит к срабатыванию сигнала тревоги.

Индуктивные средства обнаружения, в которых 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. Магнитометрические средства обнаружения предназначены для выявления попыток несанкционированного проникновения на охраняемую территорию нарушителя с ферромагнитным снаряжением. Оно фиксирует и анализирует локальные изменения постоянного магнитного поля Земли. Дополнительное поле не создается, за счет этого упомянутое средство пассивно и не обнаруживается приборами анализа. Причем имеет значение не только масса ферромагнитных предметов, но и близость их к извещателю.

Сейсмическое средство обнаружения, представляет собой систему геофонных датчиков смонтированных непосредственно в грунте, их действия основаны на сейсмических колебаниях грунта, вызываемых подвижкой почвы;

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

Инфракрасные системы охраны периметра базируются на применении оптического (инфракрасного) излучения и строятся на основе активных и пассивных инфракрасных (ИК) извещателей. Активные лучевые ИК извещатели являются двухпозиционными, они состоят из излучателя, формирующего ИК луч, и фотоприемника, расположенных в зоне прямой взаимной видимости. Сигнал тревоги формируется при прерывании луча, попадающего на блок фотоприемника, в результате пересечения его посторонним объектом. Принцип работы инфракрасного извещателя показан на рисунке 5.3

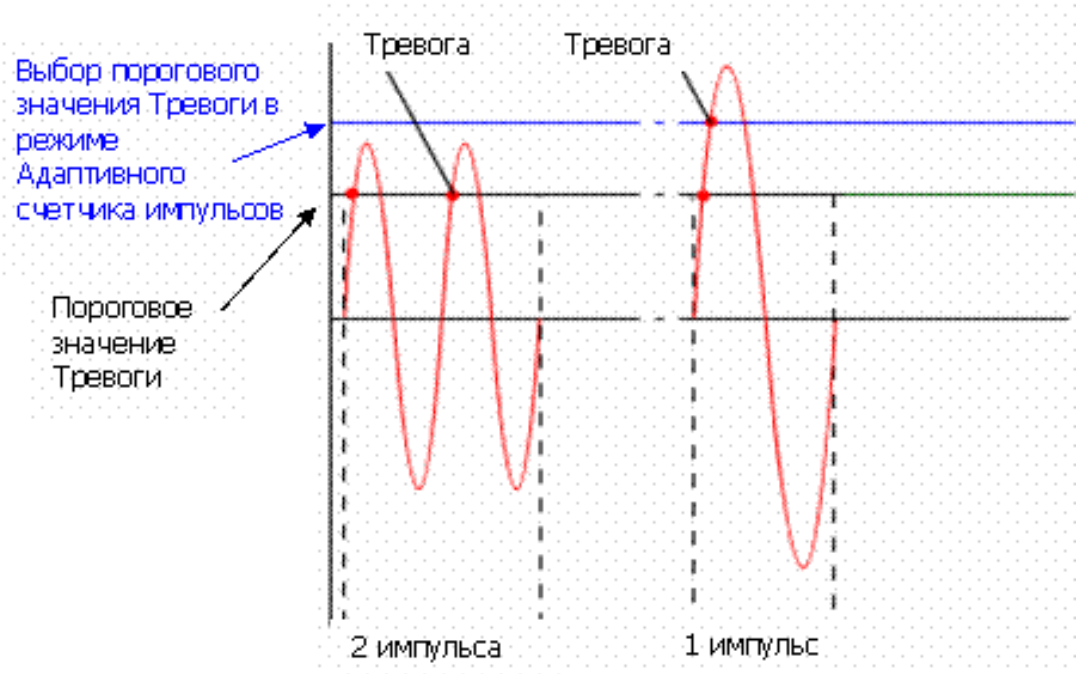


Рисунок 5.3 - Принцип работы инфракрасного извещателя

Отличительная особенность активных лучевых систем - очень узкая зона обнаружения (3-6 см), что важно для объектов, вокруг которых невозможно создать зону отчуждения.

5.2 Выбор охранных извещателей

Технические средства обнаружения — это извещатели, построенные на различных физических принципах действия. Извещатель — это устройство, формирующее определенный сигнал при изменении того или иного контролируемого параметра объекта. По области применения извещатели подразделяются на охранные, охранно-пожарные и пожарные. Охранные извещатели по виду контролируемой зоны подразделяются на точечные, линейные, поверхностные и объемные. Выбор конкретного типа извещателя определяется в зависимости от:

— сопоставления конструктивных строительных характеристик объекта, подлежащего защите, и тактико-технических характеристик извещателя;

— характера и размещения ценностей в помещениях;

— помеховой обстановки на объекте;

— вероятных путей проникновения нарушителя;

— режима и тактики охраны.

Схема выбора охранных извещателей представлена на рисунке 5.4.

Существенное влияние на выбор извещателя оказывает помеховая ситуация в районе его размещения. Помеховая ситуация может изменяться. Например, возле здания могут начаться строительные работы с использованием тяжелой техники, что создаст акустические помехи.

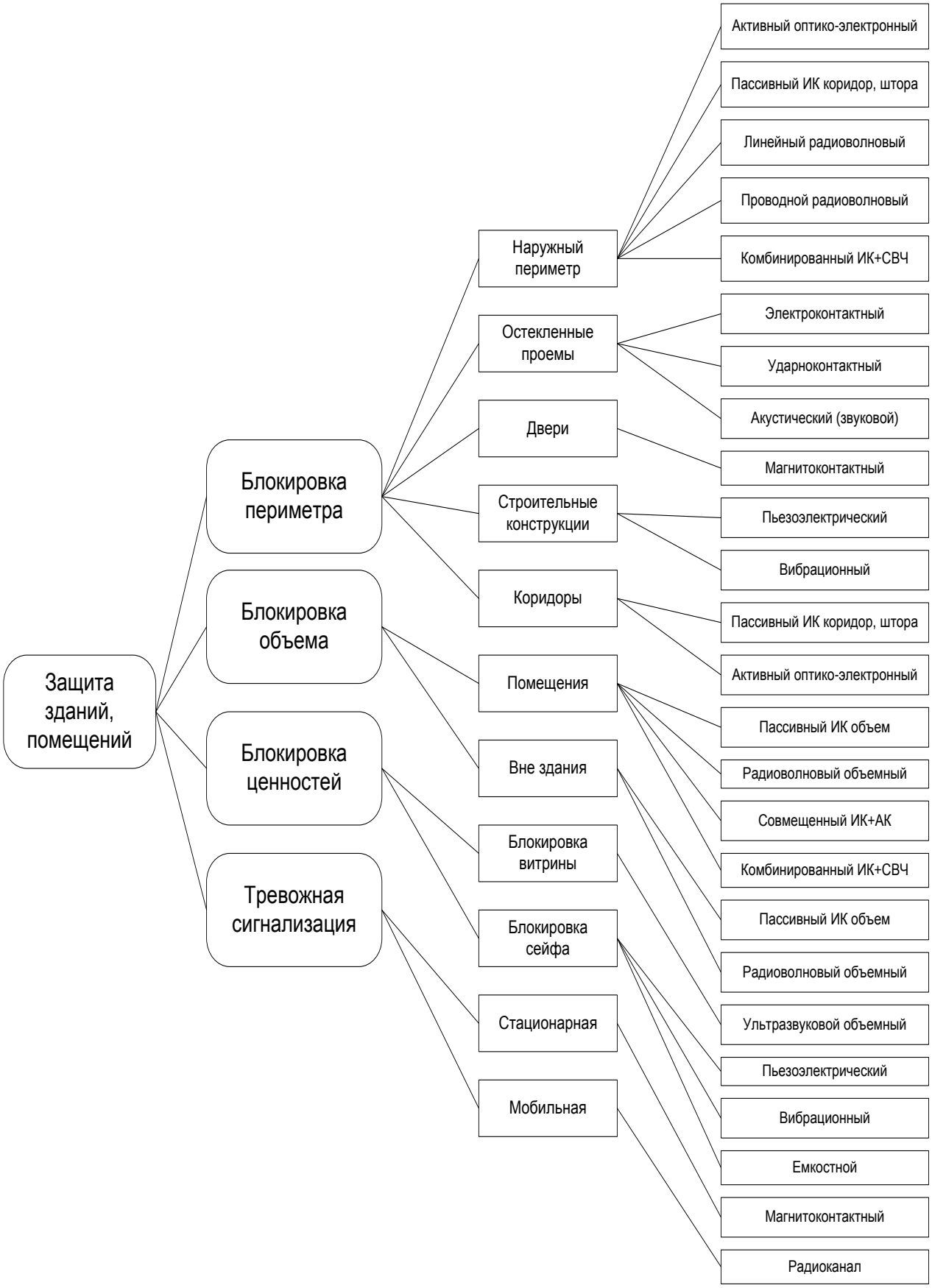


Рисунок 5.4 - Схема выбора охранных извещателей

Справочные параметры датчиков охранной сигнализации:

- вероятность правильной детекции;
- вероятность ложной тревоги;
- чувствительность датчика.

Вероятность правильной детекции Рд — вероятность того, что датчик сработает при вторжении нарушителя в охраняемую зону. Рд — величина статистическая, оценивается по результатам серии испытаний, и, как следствие, зависит от принятой методики испытаний.

В справочных данных датчика должен быть указаны внешние условия (ночь/день, облачность, время года и т.д.), модель нарушителя (ползущий, со скоростью 0,5 м/с и т.д.). Кроме того, необходимо знать методику оценки Рд. Тогда модель обнаружения описывается двумя параметрами: вероятность детекции и доверительным интервалом C_L, т.е. датчик будет обнаруживать с вероятностью Рд при уровне C_L. Отметим, что такая полная информация обычно недоступна. В большинстве случаев приходится довольствоваться значением Рд, которое следует считать условным, основанным на предположениях.

Вероятность ложной тревоги Рлт — вероятность, того, что за время Т произойдет ложное срабатывание датчика. Статистически оценивается частотой ложных тревог - количеством ложных тревог за определенный интервал времени. Средний интервал времени между двумя последовательными ложными срабатываниями называется наработкой на ложное срабатывание (Тлт). В представлении о пуассоновском характере потока ложных тревог можно записать:

$$Рлт = 1 - \exp(- tp/Тлт),$$

где: Рлт — вероятность ложной тревоги;

tp — время нахождения датчика в работоспособном состоянии.

Чувствительность — величина, обратная порогу. Порог — некое значение, ниже которого сигналы интерпретируются как шумы.

Порог регулируется во время настройки датчика. Чем больше чувствительность, тем больше вероятность детекции. Но при увеличении чувствительности возрастает и частота ложных тревог.

Таким образом, рассматривая процесс обнаружения в целом, можно выделить следующие основные показатели его качества: достоверность обнаружения; устойчивость к помехам; уязвимость к преодолению. Вероятность правильной детекции является основной характеристикой, позволяющей судить о достоверности обнаружения.

Достоверность обнаружения — это показатель качества датчика, характеризующий его способность реагировать (срабатывать) при появлении нарушителя.

Частота ложных тревог является основной характеристикой, по которой можно судить о помехоустойчивости датчика. Помехоустойчивость – это показатель качества датчика, характеризующий его способность стабильно работать в различных условиях. Проанализируем основные дестабилизирующие факторы, являющиеся причиной возникновения ложных тревог. Все они могут быть разбиты на: внутренние шумы и внешние помехи.

Внутренние шумы генерируются самой аппаратурой. Среди основных причин следует отметить следующие:

- недостатки конструктивных и схемотехнических решений;
- неправильная установка и настройка датчика;
- недостатки алгоритма обработки сигналов;
- некачественное техобслуживание.

Недостатки конструктивных и схемотехнических решений могут привести к наводкам в цепях передачи данных, например из-за плохого экранирования, плохой фильтрации, применения дешевой некачественной элементной базы. Распространенной проблемой является изменение параметров датчика при приближении к порогам допустимого температурного диапазона. Для устранения этого недостатка дополняют схемы термостабилизации параметров и т.д.

Неправильная установка датчика. Несоблюдение требований документации на прибор при монтаже датчика может привести к искажению зоны обнаружения, например при наличии препятствий для микроволновых датчиков [32].

Неправильная настройка датчика может привести к выходу зоны обнаружения датчика за пределы охраняемой зоны, особенно в помещениях со сложной конфигурацией, что приведет к срабатыванию датчика при присутствии людей в смежных комнатах. Недостатки алгоритма обработки сигналов связаны с тем, что при разработке датчика существует конфликт между целями повышения распознавания и помехоустойчивостью. Чем выше чувствительность датчика тем, выше распознавание, но и выше уровень помех. Некоторые алгоритмы не учитывают даже стандартные помехи: звонок телефона для ультразвукового датчика, восходящие тепловые потоки от батарей центрального отопления для пассивных инфракрасных датчиков и т.д.

Некачественное техобслуживание может привести, например, к запылению или загрязнению частей датчика. Крепление датчика может ослабнуть, что может привести к изменению зоны обнаружения.

Внешние помехи вызываются возмущениями среды. По происхождению их можно разделить на естественные и техногенные:

− состояние атмосферы (изменения температуры, влажности воздуха, порывы ветра, дождь, солнечная радиация и т.д.);

− электромагнитные наводки (помехи от ЛЭП, радиостанций, электропроводки);

− посторонние объекты в охраняемой зоне (птицы, мелкие животные и прочее);

− параллельная работа нескольких датчике.

Усредненное влияние помех различных типов на работу извещателей характеризуется данными таблицы 5.1.

Таблица 5.1 - Усредненное влияние помех на работу извещателей

Вид помехи	Тип извещателя				
	Аккустический	Оптико-электронный	Радиоволновой	Емкостной	Вибрационный
Внешние акустические шумы (уличные, раскаты грома и др.)	+	-	-	-	+
Внутренние (в контролируемой зоне) акустические шумы (холодильники, ТА, шум воды в трубах и др.)	+	-	-	-	-
Внешний свет (свет фар, солнечные блики)	-	+	-	-	-
Движение воздуха в помещении (сквозняки, вентиляторы, батареи отопления)	-	+	-	-	-
Движение предметов (штор, лопастей вентилятора, воды на стеклах, листьев и др.)	+	+	+	-	-
Электромагнитные помехи (сварочные аппаратыты, разряды высоковольтных линий ЛЭП, трамваев, троллейбусов, люминесцентные лампы и др.)	-	-	-	+	-
Мелкие животные, крупные насекомые	+	+	+	+	+

5.3 Характеристика пожарных извещателей

Пожарный извещателъ — устройство для формирования сигнала о пожаре. Адресный пожарный извещатель (АПИ) — техническое средство, которое передает на адресный приемно-контрольный прибор код своего адреса вместе с извещением о пожаре.

В зависимости от назначения здания, где устанавливается система пожарной безопасности, применяются и определенные датчики. Например, для

установки пожарной сигнализации в складском помещении большого метража применяются лучевые датчики. Для установки пожарной сигнализации в помещениях с большим количеством находящихся в нем людей (кинотеатры, театры, библиотеки и др.) лучше всего использовать дымовые датчики. Если мы имеем дело со складским помещением, в котором хранится, например, древесина или другие легко воспламеняющиеся природные материалы, рекомендовано применять датчики, которые реагируют на открытый огонь.

Должны учитываться мельчайшие детали помещения, в котором происходит установка пожарной сигнализации. Поскольку тепловые датчики несколько инертны при срабатывании, предпочтительней использовать датчики дымовые. На рынке пожарного оборудования существуют также комбинированные датчики. Они предназначены для оповещения о пожаре при изменении двух параметров (температурном и дымовом).

Установка пожарной сигнализации позволяет не только оповестить людей о пожаре, но и вовремя локализовать возгорание и тем самым попутно избежать материальных потерь, что тоже немаловажно. По способу приведения в действие пожарные извещатели разделяют на ручные и автоматические. В ручных извещателях отсутствует функция обнаружения очага загорания, их действие сводится к передаче тревожного извещения в электрическую цепь шлейфа сигнализации после обнаружения загорание человеком и активации извещателя путем нажатия соответствующей пусковой кнопки [36].

Автоматические пожарные извещатели работают независимо от человека. Они предназначены для обнаружения возгорания по различным анализируемым признакам и формирования извещения о пожаре при достижении контролируемого физического параметра установленного значения.

Классификация автоматических пожарных извещателей представлена на рисунке 5.5.

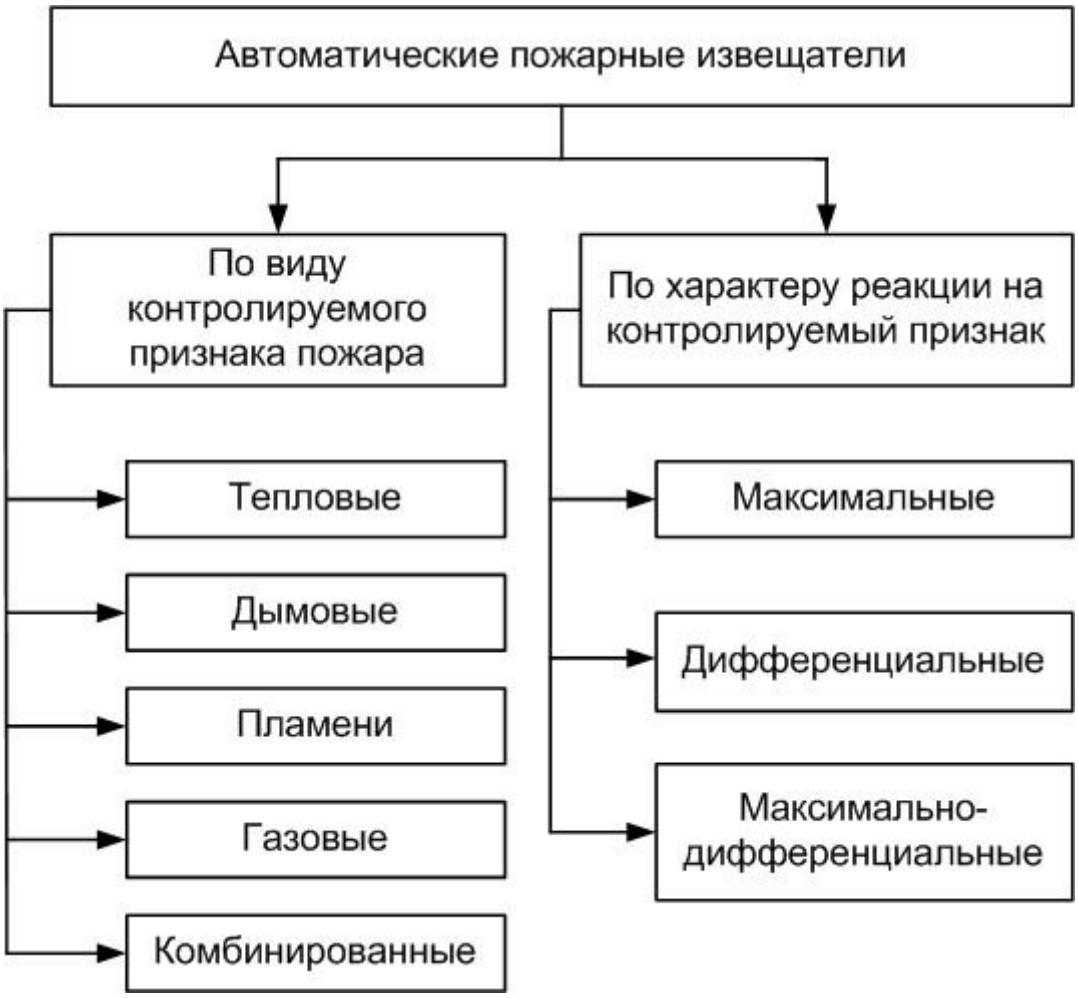


Рисунок 5.5 - Классификация автоматических пожарных извещателей

Все автоматические пожарные извещатели по характеру реакции на контролируемый признак пожара можно разделить на три группы.

К первой группе относятся извещатели максимальные. Они срабатывают при достижении контролируемым параметром установленного порога. Максимальный тепловой пожарный извещатель который создает извещение о пожаре при превышении температуры окружающей среды выше установленного порогового значения (по НПБ 85-00 «Извещатели пожарные тепловые. Технические требования пожарной безопасности. Методы испытаний»).

Ко второй группе относятся извещатели, которые реагируют на скорость нарастания контролируемого признака пожара, и называются дифференциальными. Дифференциальный тепловой пожарный извещатель

создает извещение о пожаре при превышении скорости нарастания температуры окружающей среды выше установленного порогового значения.

К третьей группе относятся извещатели, реагирующие и на достижение контролируемым параметром заданной величины порога срабатывания и на его производную, они называются максимально-дифференциальными.

По способу обнаружения пожара автоматические пожарные извещатели делят на активные и пассивные. В основу работы активных извещателей положен принцип заполнения защищаемого помещения определенным видом энергии. При пожаре в помещении фиксируется изменение создаваемого поля и выдается сигнал тревоги. Пассивные точечные извещатели реагируют на характерные информационные свойства очага пожара в месте установки извещателя.

В зависимости от способа восприятия изменения контролирующих параметров извещатели бывают точечные и линейные. Точечный пожарный извещатель (дымовой, тепловой) — пожарный извещатель, реагирующий на признаки пожара в локальной зоне. Линейный пожарный извещатель (дымовой, тепловой) — пожарный извещатель, реагирующий на факторы пожара в протяженной, линейной зоне.

Адресным пожарным извещателем называют извещатель, который передает на приемно-контрольный прибор код своего адреса.

Автономный пожарный извещатель — пожарный извещатель, реагирующий на определенный уровень концентрации аэрозольных продуктов горения веществ и материалов и других признаков пожара, в корпусе которого конструктивно объединены автономный источник питания и компоненты, необходимые для обнаружения пожара и передачи сообщения о нем.

Тепловые и дымовые пожарные извещатели получили наибольшее распространение в автоматических системах пожарной сигнализации. Это связано со спецификой начальной фазы процесса горения большинства пожароопасных веществ, а также относительной простотой схемных решений этих извещателей.

В **тепловых пожарных извещателях** широко используется термоэлектрический эффект, явления изменения при определенных температурах магнитных свойств ферромагнитных материалов, механических свойств легкоплавких спаев, электропроводности полупроводниковых материалов, линейных размеров металлов и др. Тепловые пожарные извещатели наиболее эффективны когда определяющим фактором пожара является тепловыделение.

Точечные тепловые пожарные извещатели максимального действия, чувствительным элементом которых являются герконовые реле, температурное реле на основе «эффекта памяти металла», а также иные контактные извещатели недороги, но обладают значительной инерционностью, они срабатывают при достижении на защищаемом объекте определённой температуры, и не позволяют обнаружить пожар в первоначальной стадии развития. В связи с этим в настоящее время производство наиболее дешёвых тепловых пожарных извещателей максимального действия типа резко сокращено и применение ограничено.

Необходимость обнаруживать пожары в ранней стадии и в любой точке по длине защищаемого объекта привела к созданию термокабелей, которые представляют собой по существу непрерывный, распределенный по длине объекта пожарный извещатель. Созданные и используемые в промышленности образцы термокабелей (например, «Алармлайн», «Протектовейер») генерируют предупредительный или аварийный сигнал при нагреве воздушной среды до температуры, соответствующей плавлению изоляции металлических жил термокабеля.

Примером линейного теплового пожарного извещателя является линейная система сигнализации Alarmline LHD 4 фирмы “KIDDE”. Устройство обнаружения пожара имеет сенсорную длину чувствительного элемента 300 м (максимальная длина 1,5 км), слабо чувствительного по отношению к механическим и химическим воздействиям, коррозии, влажности, пыли и пригодного для применения во взрывоопасных зонах. Применение линейных

тепловых пожарных извещателей наиболее эффективно в кабельных каналах, электроподстанциях, высокостеллажных складах, морских судах, ангарах, фальшполах компьютерных залов, в транспортных тоннелях. Линейный извещатель точно определяет местонахождение точки перегрева, в любом месте этих сооружений, а также выдерживает агрессивное воздействие окружающей среды.

Дымовые пожарные извещатели по принципу действия бывают ионизационные (радиоизотопные) и фотоэлектрические.

Радиоизотопные дымовые пожарные извещатели (ИП 211) построены на основе дымовой камеры, в которой находятся два электрода (анод и катод) и капсулы с радиоактивным элементом (плутоний, америций). В дежурном режиме воздух в камере ионизирован и между электродами возникает ионизационный электрический ток. Если в камеру попадают частицы дыма, степень ионизация уменьшается и ток между электродами равен нулю. При этом блок обработки сигналов улавливает изменение тока и вырабатывает сигнал «Пожар». К достоинствам этих извещателей можно отнести практически одинаковую способность реагировать как на светлый, так и на темный дым.

Фотоэлектрические дымовые пожарные извещатели (ИП 212) делятся на точечные и линейные.

В точечных фотоэлектрических дымовых пожарных извещателях используется принцип действия, заключающийся в регистрации оптического излучения, отраженного от частиц дыма, попадающих в дымовую камеру извещателя. Точечные фотоэлектрические дымовые пожарные извещатели имеют высокую чувствительность к светлому и серому дыму, но обладают несколько худшей чувствительностью к темному дыму, который плохо отражает электромагнитное излучение источника света.

Устройство линейных дымовых пожарных извещателей основано на принципе ослабления электромагнитного потока между источником излучения и фотоприемником под воздействием частиц дыма. Прибор такого типа состоит из двух блоков, один из которых содержит источник оптического излучения, а

другой – фотоприемник. К достоинствам линейных дымовых извещателей можно отнести большую дальность действия (до 100 м). Линейные дымовые пожарные извещатели хорошо реагируют как на темный, так и на серый дым.

К недостаткам следует отнести необходимость прямой видимости между источником и фотоприемником и накопление пыли на линзовой оптике или защищающих конструктивных элементах.

Производятся также аспирационные дымовые пожарные извещатели. Основное отличие аспирационных дымовых пожарных извещателей от обычных дымовых состоит в том, что имея в своём составе вентилятор (аспиратор), через дымовую камеру извещателя постоянно прокачивается и анализируется воздух из защищаемого помещения. Забор проб воздуха из помещений осуществляется через систему трубопроводов имеющую калиброванные всасывающие отверстия. Такая система забора воздуха позволяет повысить чувствительность аспирационного извещателя по сравнению с обычными от 100 до 300 раз.

Использования аспирационных извещателей показывает, что чувствительность и помехозащищенность таких извещателей выше чем у традиционных точечных оптико-электронных дымовых пожарных извещателей.

Пожарные извещатели пламени. Для обнаружения быстроразвивающихся пожаров на начальной стадии наиболее эффективны извещатели пламени. Важными особенностями использования извещателей пламени является то, что обнаружение излучения очага пожара на излучающем фоне требует специальных мероприятий по защите от ложных срабатываний. Излучающий фон может насытить чувствительный элемент извещателя, и излучение помехи небольшой интенсивности вызывает срабатывание извещателя. Поэтому в пожарных извещателях пламени используются чувствительные элементы имеющие избирательную спектральную характеристику.

Извещатель пламени пожарный – прибор, реагирующий на электромагнитное излучение пламени или тлеющего очага (НПБ 72-98). Чувствительный элемент – преобразователь электромагнитного излучения в электрический сигнал – реагирующий на электромагнитное излучение пламени в инфракрасном или ультрафиолетовом диапазоне длин волн, в соответствии со спектром электромагнитного излучения.

Многодиапазонные извещатели – это приборы, реагирующие на электромагнитное излучение пламени в двух или более участках спектра.

В ультрафиолетовом диапазоне спектра применяются счетчики фотонов или газонаполненные индикаторы. Эти элементы обладают большей чувствительностью и работают по принципу внешнего фотоэффекта. Элементы работают в импульсном режиме и электронные схемы построены по принципу обработки информации о количестве поступающих импульсов от очага пожара.

Инфракрасные извещатели в качестве чувствительных элементов используют фоторезисторы или фотодиоды. Они работают по принципу внутреннего фотоэффекта и изменяют электрические параметры в зависимости от интенсивности падающего на них светового потока. Схемы обработки сигнала носят аналоговый характер. Их помехозащищенность от посторонних источников света осуществляется несколькими способами: изменением чувствительности, оптической фильтрацией, а также электрической фильтрацией.

Газовые пожарные извещатели.

Дымовые и тепловые извещатели срабатывают когда контролируемый параметр достигнет чувствительного элемента извещателя. Но бывают случаи, когда наличие вентиляции, кондиционирования воздуха, особенности архитектурной планировки, сложная конфигурация размещения оборудования и материалов и т.д., приводят к увеличению суммарного времени обнаружения пожара, что в свою очередь может создать реальную угрозу жизни и здоровья человека, экологической опасности, техногенным катастрофам и другим опасным факторам. В этих случаях незаменимы газовые пожарные извещатели.

Извещатель пожарный газовый – прибор, реагирующий на газы, выделяющиеся при тлении или горении материалов (по НПБ 71-98).

Газовые извещатели контролируют химический состав воздуха, который изменяется из-за термического разложения, пиролиза, перегретых и начинающих тлеть горючих материалов. Именно на этой стадии развития пожара можно принять адекватные меры его тушения, а в случае перегрева приборов и оборудования их можно отключить автоматически по сигналу с газового извещателя, ликвидировав тем самым развивающуюся пожарную опасность в самой ранней ее стадии развития. Испытания показали, что по сравнению со стандартными дымовыми извещателями, быстродействие газовых увеличилось в 10–20 раз, а чувствительность увеличилась более чем в 100 раз. Газовых извещатели не боятся пыли и конденсата влаги, хороший эффект дает встраивание их в системы вентиляции.

Комбинированные пожарные извещатели (КПИ)

Основными классификационными признаками КПИ являются вид контролируемых факторов пожара и принципы действия каналов обнаружения. Данные признаки отражены в условном обозначении и указываются в технической документации на извещатель. При объединении нескольких каналов обнаружения применяют различные алгоритмы анализа признаков пожара и принятия решения о дальнейших действиях. Наиболее широко используется сочетание дымового и теплового каналов обнаружения. На некоторых объектах при возникновении пожара рост температуры происходит быстрее, чем дымообразование, применение дымо-теплового КПИ с дифференциальным тепловым каналом позволит значительно уменьшить время реагирования и обнаружить очаг возгорания в несколько раз меньший по тепловой мощности, чем по дыму. Иногда дополнительно может применяться и газовый канал.

6 Системы охранно-пожарной сигнализации

Охранно-пожарная сигнализация, согласно ГОСТ 26342-84 — это получение, обработка, передача и представление в заданном виде потребителям при помощи технических средств информации о проникновении на охраняемые объекты и о пожаре на них.

Система охранно-пожарной сигнализации (ОПС) предназначена для защиты помещения от возгорания и/или несанкционированного проникновения нарушителя.

Охранно-пожарная сигнализация интегрируется в комплекс, объединяющий системы безопасности и инженерные, коммуникационные системы объекта, обеспечивая достоверной информацией технические системы оповещения, пожаротушения, контроля доступа, дымоудаления и др.

6.1 Структура охранно-пожарной сигнализации

Система охранно-пожарной сигнализации является системой сбора и анализа данных о состоянии объекта. Информация о состоянии объекта, снимаемая с помощью различных датчиков-анализаторов, непрерывно обрабатывается приемно-контрольной панелью – центральным пунктом системы ОПС [35]. Подсистема охранной сигнализации обрабатывает следующие параметры:

— состояние контактов магнитоконтактных датчиков (открыто-закрыто);

— сигналы о нарушении объема помещения;

— сигналы о пересечении периметра.

Сигналы, поступающие на подсистему пожарной сигнализации:

— температура внутри помещения;

— уровень задымления;

— излучение открытого пламени.

Типовая структура ОПС представлена на рисунке 6.1.

Рисунок 6.1 – Типовая структура ОПС

Каналом передачи информации является шлейф сигнализации – двухпроводная или четырехпроводная линия связи. На рисунке 6.1 цифрой 1 отмечен пожарный шлейф, а цифрой 2 – охранный шлейф. Шлейф является также мерой группировки информации и позволяет разбить охраняемый объект на зоны. Информация о значении вышеперечисленных параметров обрабатывается приемно-контрольной панелью, являющейся центральным узлом сбора информации. В зависимости от настроек и алгоритма работы при нарушении шлейфа или превышении порогового значения одного из параметров приемно-контрольная панель (ПКП) формирует сигналы для запуска исполнительных устройств. На рисунке 6.1 цифрой 3 отмечен сигнал для запуска системы оповещения о пожаре, а цифрой 4 – запуск системы передачи извещений на пульт централизованного наблюдения.

Охранные и пожарные извещатели были рассмотрены в предыдущих разделах учебного пособия. Важным звеном ОПС является приемно-контрольная панель или прибор приемно-контрольный охранно-пожарный.

6.2 Характеристика приемно-контрольного прибора

Приборы приемно-контрольные и контрольные панели относятся к техническим средствам контроля и регистрации информации. Они предназначены для непрерывного сбора информации от извещателей, включенных в шлейф сигнализации, анализа тревожной ситуации на объекте, формирования и передачи извещений о состоянии объекта на пульт централизованного наблюдения, а также управления местными световыми и звуковыми оповешателями и индикаторами. Кроме того, приборы обеспечивают сдачу и снятие объекта с охраны по принятой тактике, а в ряде случаев — электропитание извещателей.

Приборы являются основными элементами, формирующими на объекте информационно-аналитическую систему охранной или охранно-пожарной сигнализации. Такая система может быть автономной или централизованной. При автономной охране приборы устанавливаются в помещении (пункте) охраны, размещаемом на охраняемом объекте или в непосредственной близости от него. При централизованной охране объектовый комплекс технических средств, формируемый одним или несколькими приборами, образует объектовую подсистему охранно-пожарной сигнализации, которая с помощью системы передачи извещений передает в заданном виде информацию о состоянии объекта на пульт централизованного наблюдения, размещаемый в центре приема извещений о тревоге (пункте централизованной охраны). Информация, формируемая прибором, как при автономной, так и централизованной охране передается сотрудникам специальных служб обеспечения охраны объекта, на которых возложены функции реагирования на тревожные извещения, поступающие с объекта.

Классификация ПКП приведена на рисунке 6.2.

Рисунок 6.2 - Классификация ПКП

Шлейф сигнализации является одной из необходимых составных частей объектовой системы охранно-пожарной сигнализации. Он представляет собой проводную линию, электрически связывающую выносной элемент, выходные цепи охранных, пожарных и охранно-пожарных извещателей со входом приемноконтрольного прибора. Шлейф охранно-пожарной сигнализации — это электрическая цепь, предназначенная для передачи на прибор приемно-контрольный тревожных и служебных извещений от извещателей, а также (при необходимости) для подачи на извещатели электропитания. Шлейф сигнализации, как правило, двухпроводный; он включает в себя выносные (вспомогательные) элементы, устанавливаемые в конце электрической цепи.

Для выбора приемно-контрольной панели сначала необходимо определить тип используемой ОПС (пороговая, адресно-аналоговая, комбинированная).

Аналоговые (неадресные) системы строятся по следующему принципу. Охраняемый объект разбивается на области прокладкой отдельных шлейфов, объединяющих некоторое количество извещателей. При срабатывании любого датчика подается сигнал тревоги по всему шлейфу. Решение о возникновении события «принимает» только извещатель, работоспособность которого можно проверить только во время технического обслуживания ОПС. Недостатками таких систем являются высокая вероятность ложных срабатываний, локализация сигнала с точностью до шлейфа, ограничение контролируемой зоны. Стоимость такой системы относительно низкая, хотя и необходимо прокладывать большое количество шлейфов. Задачи централизованного управления выполняет охранно-пожарная панель. Применение аналоговых систем возможно на всех типах объектов. Но при большом количестве областей тревоги возникает необходимость большого объема работ по монтажу проводных коммуникаций.

Адресные системы предполагают монтаж на одном шлейфе сигнализации адресных датчиков. Такие системы позволяют заменить многожильные кабели, соединяющие извещатели с приемно-контрольным прибором (ПКП) на одну пару проводов шины данных.

Адресные неопросные системы являются, по сути, пороговыми, дополненными лишь возможностью передачи кода адреса сработавшего извещателя. Этим системам присущи все недостатки аналоговых – невозможность автоматического контроля работоспособности пожарных извещателей (при любом отказе электроники связь извещателя с ПКП прекращается).

Адресные опросные системы осуществляют периодический опрос извещателей, обеспечивают контроль их работоспособности при любом виде отказа, что позволяет устанавливать по одному извещателю в каждом помещении вместо двух. В адресных опросных ОПС могут быть реализованы сложные алгоритмы обработки информации, например, автокомпенсация

изменения чувствительности извещателей с течением времени. Снижается вероятность ложных срабатываний. Например, адресный датчик разбития стекла, в отличие от безадресного, укажет, какое именно окно было разбито.

Самым перспективным направлением в области построения систем сигнализации являются **комбинированные (адресно-аналоговые) системы.** Адресно-аналоговые извещатели измеряют величину задымленности или температуру на объекте, а сигнал формируется на основании математической обработки полученных данных в ПКП (специализированная ЭВМ). Есть возможность подключать любые датчики, система способна определить их тип и требуемый алгоритм работы с ними, даже если все эти устройства включены в один шлейф охранной сигнализации. Эти системы обеспечивают максимальную скорость принятия решений и управления [1]. Для правильной работы адресно-аналоговой аппаратуры необходимо учитывать уникальный для каждой системы язык общения ее компонентов (протокол). Применение этих систем дает возможность быстро, без больших затрат внести изменения в уже существующую систему при изменении и расширении зон объекта. Структура ПКП представлена на рисунке 6.3.

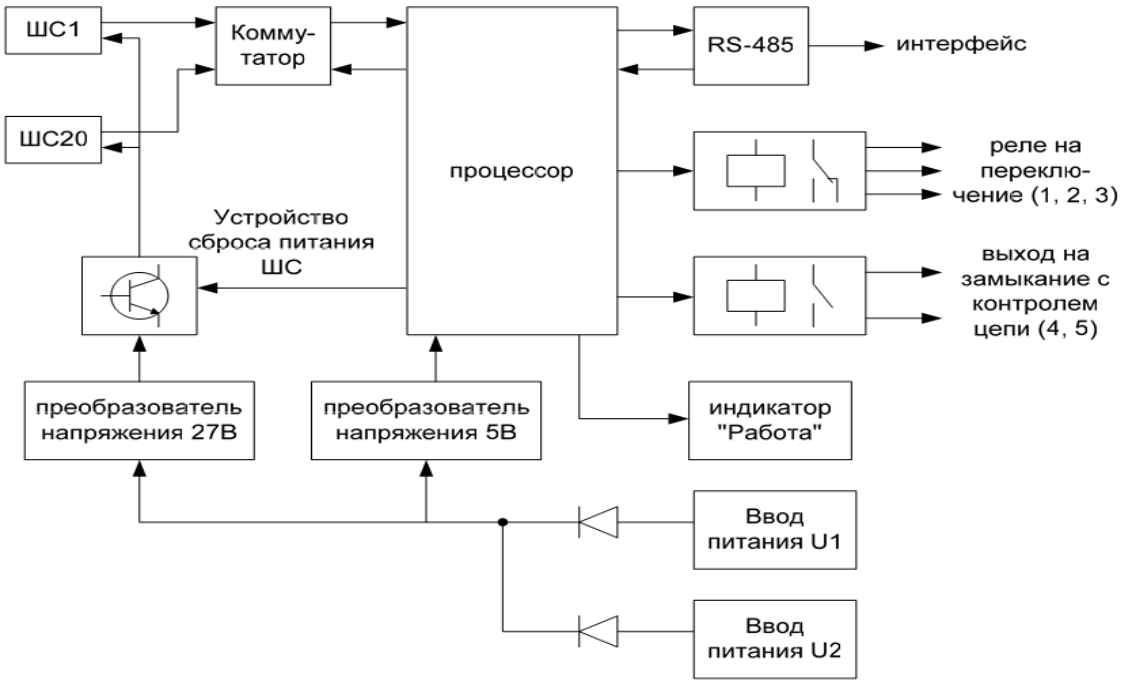


Рисунок 6.3 - Структура ПКП

Количество шлейфов сигнализации – важнейший параметр ПКП. Выпускаются приборы с количеством шлейфов от 1 до 40. Если для охраны объекта недостаточно шлейфов одного ПКП, то необходимо проектировать модульную систему ОПС, которая характеризуется тем, что приборы ОПС связаны сетевым интерфейсом (RS-485, а для связи с ЭВМ – RS-232, Ethernet).

К приемно-контрольной панели для функций оповещения подключаются световые и звуковые оповещатели. Они могут быть как встроенными в ПКП, так и внешними (выносными). Также любой ПКП содержит блок реле, которые можно запрограммировать на срабатывание какого-либо шлейфа или группы шлейфов сигнализации. Типы контактов реле могут быть на замыкание, переключение. Через цепи реле могут подключаться устройства передачи извещений пожар/тревога на пульт пожарной части или пульт централизованного наблюдения по телефонной линии или радиоканалу.

6.3 Характеристика систем оповещения

Системы оповещения могут быть в составе охранных, пожарных и охранно-пожарных систем. Соответственно основные функции таких систем – выдача сигнала о проникновении нарушителя либо возникновении пожара на объекте.

Основной способ обеспечения безопасности людей при пожарах в общественных зданиях и сооружениях — это их эвакуация в безопасную зону. Безопасной зоной считаются помещения (участки) внутри зданий и пространство снаружи здания, где исключается воздействие опасных факторов пожара на людей.

Система оповещения и управления эвакуацией (СОУЭ) – комплекс организационных мероприятий и технических средств, предназначенный для своевременного сообщения людям информации о возникновении пожара и (или) необходимости и путях эвакуации.

Зона пожарного оповещения – часть здания, где проводится одновременное и одинаковое по способу оповещение людей о пожаре.

Технические средства оповещения – звуковые, речевые, световые и комбинированные пожарные оповещатели, приборы управления ими, а также эвакуационные знаки пожарной безопасности.

Статический указатель – эвакуационный знак пожарной безопасности с постоянным смысловым значением. Динамический указатель – эвакуационный знак пожарной безопасности с изменяемым смысловым значением. Автоматическое управление – приведение в действие СОУЭ командным импульсом автоматических установок пожарной сигнализации или пожаротушения. Полуавтоматическое управление – приведение в действие СОУЭ диспетчером при получении командного импульса от автоматических установок пожарной сигнализации или пожаротушения.

Эвакуация обеспечивается согласно ГОСТ 12.1.004 — 91 посредством устройства необходимого количества эвакуационных путей и соблюдения их требуемых параметров, а также организацией своевременного оповещения людей и управления их движением. Назначение систем оповещения и управления эвакуацией людей:

— своевременно передавать информацию о возникновении пожара,

— способствовать реализации плана эвакуации людей с объекта.

На небольших объектах в качестве устройств управления СОУЭ данных типов используются приборы приемно-контрольные или контрольные панели охранно-пожарной сигнализации, но, как правило, мощности для питания приборов оповещения у большинства ППК ограничены. Для решения этой проблемы при осуществлении функций оповещения на небольших объектах используют исполнительные реле ППК (в качестве схем управления) и бесперебойные источники питания систем (в качестве приборов, питающих шлейфы оповещателей). Необходимо помнить о выполнении обязательных требованиях НПБ: осуществление функций аппаратного контроля целостности

линий (шлейфов) оповещателей, а также контролируемой работоспособности управляющих и питающих устройств.

6.3.1 Типы пожарных оповещений

При определении типа СОУЭ и выборе оборудования для ее проектирования необходимо руководствоваться нормативными документами, утвержденными в установленном законом порядке. В первую очередь, это НПБ 77-98 (Нормы пожарной безопасности), устанавливающие общие технические требования к техническим средствам оповещения и управления эвакуацией, и НПБ 104-03, устанавливающие требования пожарной безопасности к СОУЭ, а также их типы с определением перечня объектов, подлежащих оснащению такими системами.

В зависимости от функциональных характеристик СОУЭ подразделяются на пять типов, указанных в таблице 6.1.

Таблица 6.1 – Типы пожарных оповещений

Описание оповещающих сигналов	№ типа оповещения
Звуковое оповещение (звонки, тонированный сигнал и др.).	1
Звуковое оповещение и светоуказатели «Выход». Оповещение должно производиться во всех помещениях одновременно.	2
Речевое оповещение и наличие светоуказателей «Выход». Регламентируется очередность оповещения: сначала обслуживающего персонала, а затем всех остальных по разработанной очередности.	3
Речевое оповещение, наличие светоуказателей направления движения и «Выход». Должна обеспечиваться связь зоны оповещения с диспетчерской. Регламентируется очередность оповещения.	4
Речевое оповещение, наличие светоуказателей направления движения и «Выход». Светоуказатели направления движения должны быть с раздельным включением для каждой зоны. Должна обеспечиваться связь зоны оповещения с диспетчерской. Регламентируется очередность оповещения.	5

Требования настоящих норм при выборе оборудования и проектировании систем оповещения являются обязательными. Для большинства небольших и средних объектов нормами пожарной безопасности определена установка СОУЭ 1-го и 2-го типов.

6.3.2 Классификация охранно-пожарных оповещателей

Охранный оповещатель – это техническое средство охранной сигнализации, предназначенное для оповещения о возникновении криминальной угрозы на охраняемом объекте. Пожарный оповещатель предназначен для своевременной передачи информации о возникновении пожара и реализации плана эвакуации людей с объекта. Классификация оповещателей пожарно-охранной сигнализации представлена на рисунке 6.4.

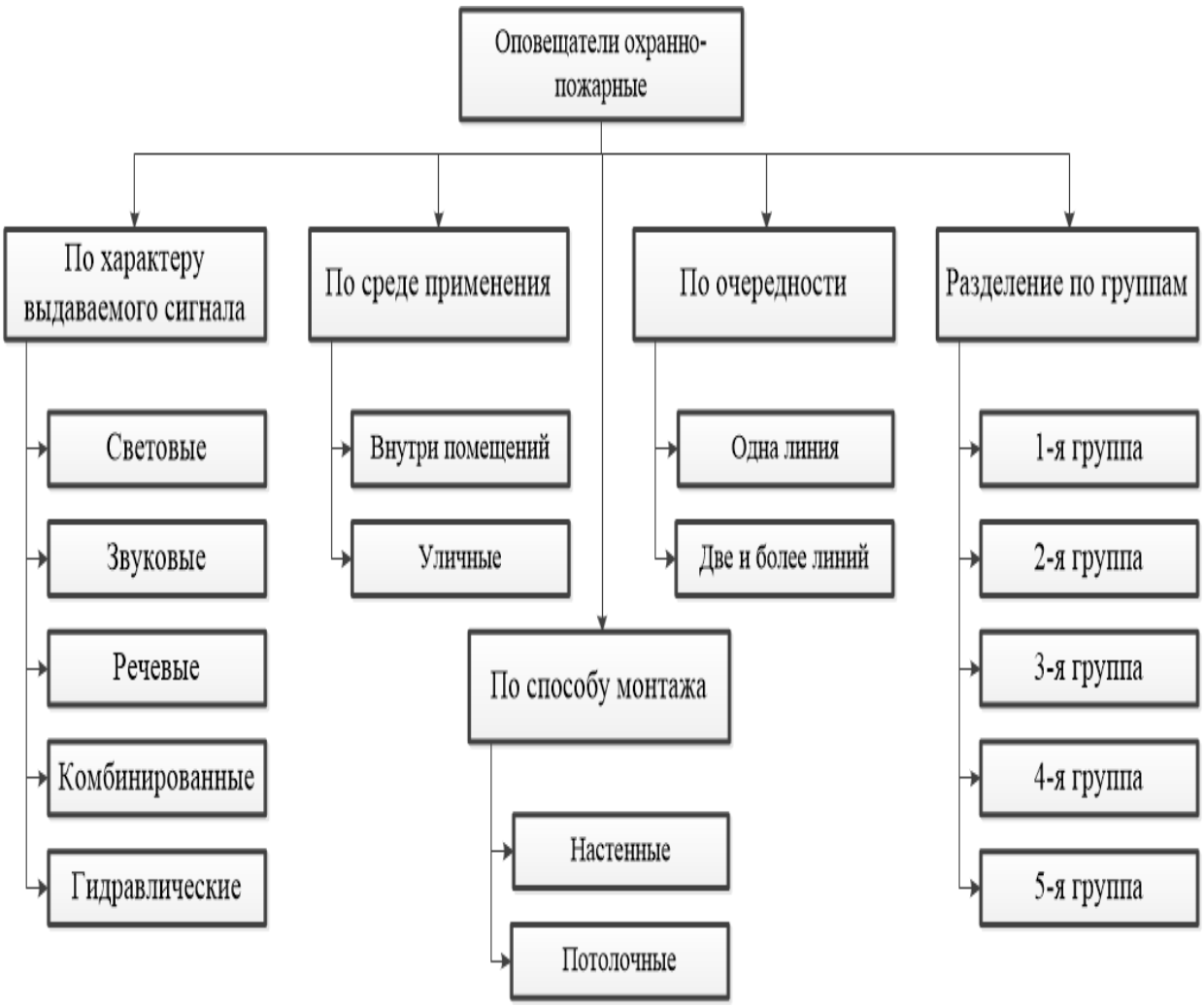


Рисунок 6.4 – Классификация охранно-пожарных оповещателей

Классификация, общие технические требования и методы испытаний охранных оповещателей указаны в ГОСТ Р 54126-2010. Все оповещатели служат для подачи звукового или светового сигнала для привлечения внимания охраны и психологического воздействия на нарушителя. В световых оповещателях используются лампы накаливания, светодиоды или импульсные источники света. В качестве звуковых используются электромагнитные сирены и звонки, электродинамические громкоговорители и сирены, пьезоэлектрические сирены. В качестве речевых используются громкоговорители. Комбинированные - это два разных оповещателя в одном корпусе.

Структура группы символов обозначения для оповещателей должна быть следующей:

X1X2X3 - X4/X5X6

X4- порядковый номер разработки оповещателя, регистрируемый соответствующим государственным органом, ответственным за проведение технической политики в данной сфере;

X5 - обозначение модификации (первая модификация - А, вторая - Б и т.д.);

X6 - обозначение модернизации (первая модернизация - 1, вторая - 2 и т.д.)

Пример условного обозначения: ОО "Сова" К3а-5/А1.

Оповещатель охранный комбинированный, для размещения на открытом воздухе, без встроенного источника электропитания, порядковый номер разработки 5, модификация А, с наименованием "Сова", первой модернизации

Звуковые оповещатели должны иметь расширенную информативность, т.е. кроме тревожного сигнала должны выдавать информационные сигналы для индикации состояния ППК, например: "Взятие под охрану", "Снятие с охраны", "Отметка наряда" и др. Вид этих сигналов должен отличаться от сигнала "Тревога".

Параметры сигналов звуковых оповещателей должны соответствовать ГОСТ 21786. Требования устойчивости к воздействию механических факторов устанавливают в технических условиях на оповещатели конкретного типа в соответствии с условиями эксплуатации и группами исполнения изделий по ГОСТ 16962.

Основной трудностью при проектировании систем оповещения является правильный подбор количества, мощности включения и оптимальное расположение оповещателей в помещениях. Места установки оповещателей должны выбираться из расчета достижения максимальной слышимости и разборчивости передаваемой информации.

В качестве примера приведем оповещатель охранно-пожарный комбинированный МАЯК-12-КП. Он предназначен для светового и звукового оповещения о состоянии объекта, охраняемого с помощью приборов охранно-пожарной сигнализации. Характеристики представлены в таблице 6.2.

Таблица 6.2 - Характеристики оповещателя МАЯК-12-КП

Параметр	Значение
Диапазон рабочих температур, °С	-30 … +55
Габаритные размеры, мм	80x80x42
Напряжение питания постоянного тока, В	10,8 … 13,2
Ток потребления светового оповещателя, мА	25
Ток потребления звукового оповещателя, мА	50
Уровень громкости звукового сигнала оповещения, дБ	100
Номинальное время непрерывной работы оповещателя в режиме «Тревога», мин.	60

7 Практические задания

7.1 Практическая работа № 1. Характеристика объекта защиты

Цель. Анализ структуры, деятельности и защищаемых ресурсов объекта. Категорирование объекта защиты.

Задачи.

1 Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта.

2 Определение содержания и местонахождения защищаемых ресурсов на объекте.

3 Построение плана объекта. Определение защищаемых зон на плане.

4 Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты.

5 Построение структурной модели защищаемой информации.

6 Определение категории защищаемого объекта.

Задание 1. Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта.

Структура подразделений объекта может быть представлена в виде схемы или таблицы. Под организационной структурой предприятия понимаются состав, соподчиненность, взаимодействие и распределение работ по подразделениям и органам управления, между которыми устанавливаются определенные отношения по поводу реализации властных полномочий, потоков команд и информации. Организационная структура объекта построена по линейно-функциональному признаку.

В качестве примера рассмотрим объект информатизации больница. Руководителем является главный врач. В подчинении у главного врача находятся заместитель по медицинской части, заместитель по экономическим

вопросам, главный бухгалтер, начальник отдела кадров, заместитель главного врача архиватор и информационно вычислительный центр и служба охраны, включающая в себя руководителя охраны помещений, руководителя пожарной охраны и штат охранников. Главный врач контролирует работу управлений, которым подчинены различные отделы. Каждый отдел подчиняется начальнику отдела. Организационная структура объекта показана на рисунке 7.1.

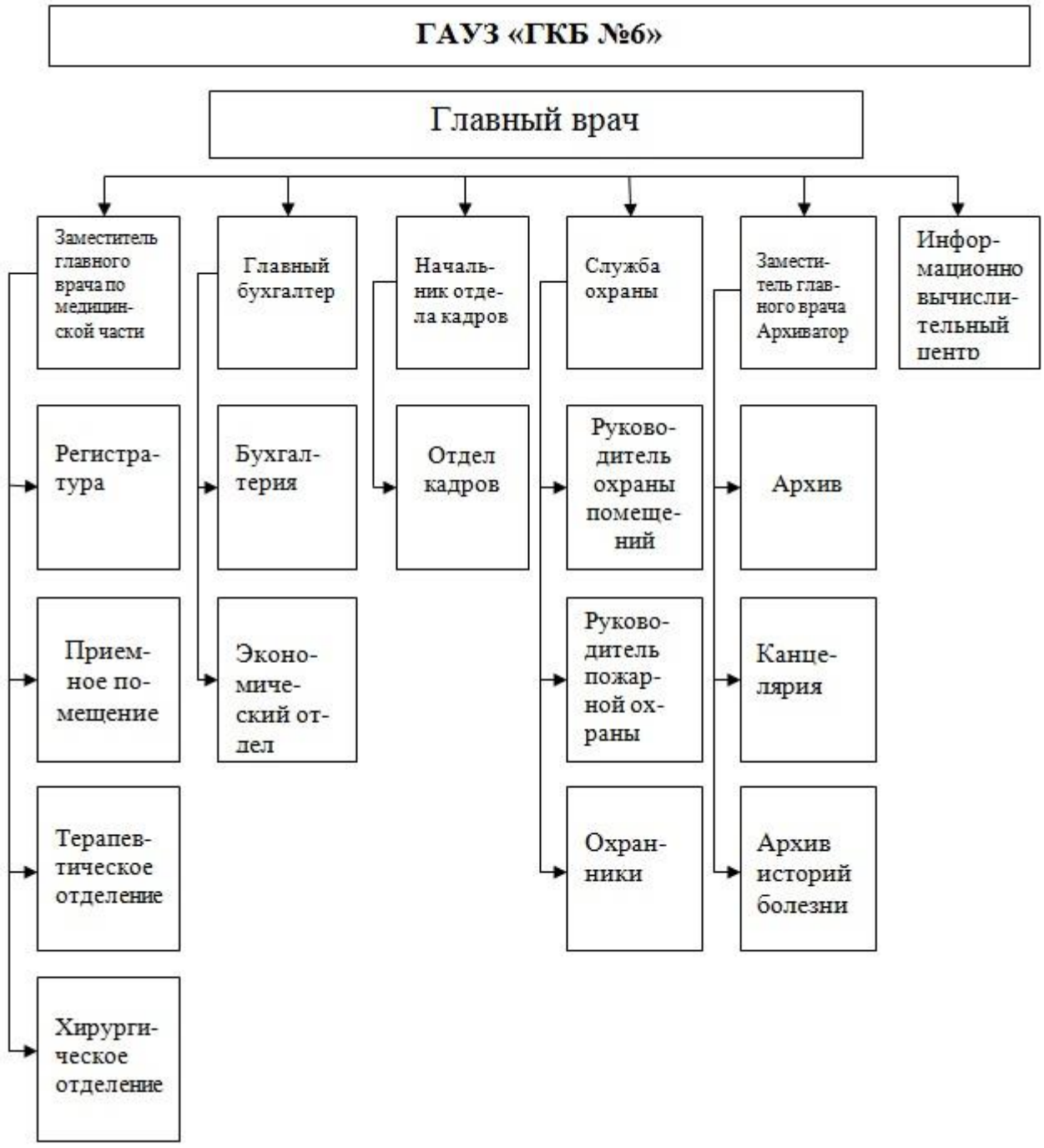


Рисунок 7.1 - Пример организационной структуры объекта

Далее необходимо перечислить решаемые задачи и направления деятельности, осуществляемой на объекте. Привести описание ведущихся на объекте работ, дать характеристику операций, выполняемых на объекте и условий их выполнения. Сформулировать назначение объекта.

Определение функционально-отраслевой принадлежности объекта. По назначению все объекты информатизации делятся на:

- производственные;
- строительные;
- транспортные;
- топливно-энергетического комплекса;
- оборонно-промышленного комплекса;
- социального назначения;
- культурного назначения.

Определить к какому типу относится заданный объект. Определить виды и масштабы возможного ущерба в результате нарушения безопасности. Определить категорию заданного объекта по уровню важности в соответствии с ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации».

Задание 2. Определение содержания и местонахождения защищаемых ресурсов на объекте. Пример приведен в таблице 7.1.

Таблица 7.1 - Основные объекты защиты ГАУЗ «ГКБ № 6»

Объект защиты	Место расположения
Персонал, пациенты	Основное здание больницы и прилегающая к ней территория
Здания, сооружения	Территория предприятия
Конфиденциальная информация	Регистратура, кабинеты больницы
Носители конфиденциальной информации: документы, содержащие ПДн, служебную и коммерческую информацию	Основное здание больницы (кабинеты 5,6,3)
Оборудование и медтехника	кабинеты 3,4
Средства вычислительной техники	Кабинеты 3,4,5,6
Финансовые ценности	Кабинет руководителя (кабинет 2)
Фармацевтические препараты	Аптека больницы

Задание 4. Построение плана объекта. Определение защищаемых зон на плане. Построить план объекта, с помощью принятых стандартом условных обозначений показать все объекты защиты. Определить категории защищаемых зон. Определить структуру контролируемых зон. Пример плана объекта показан на рисунке 7.2.

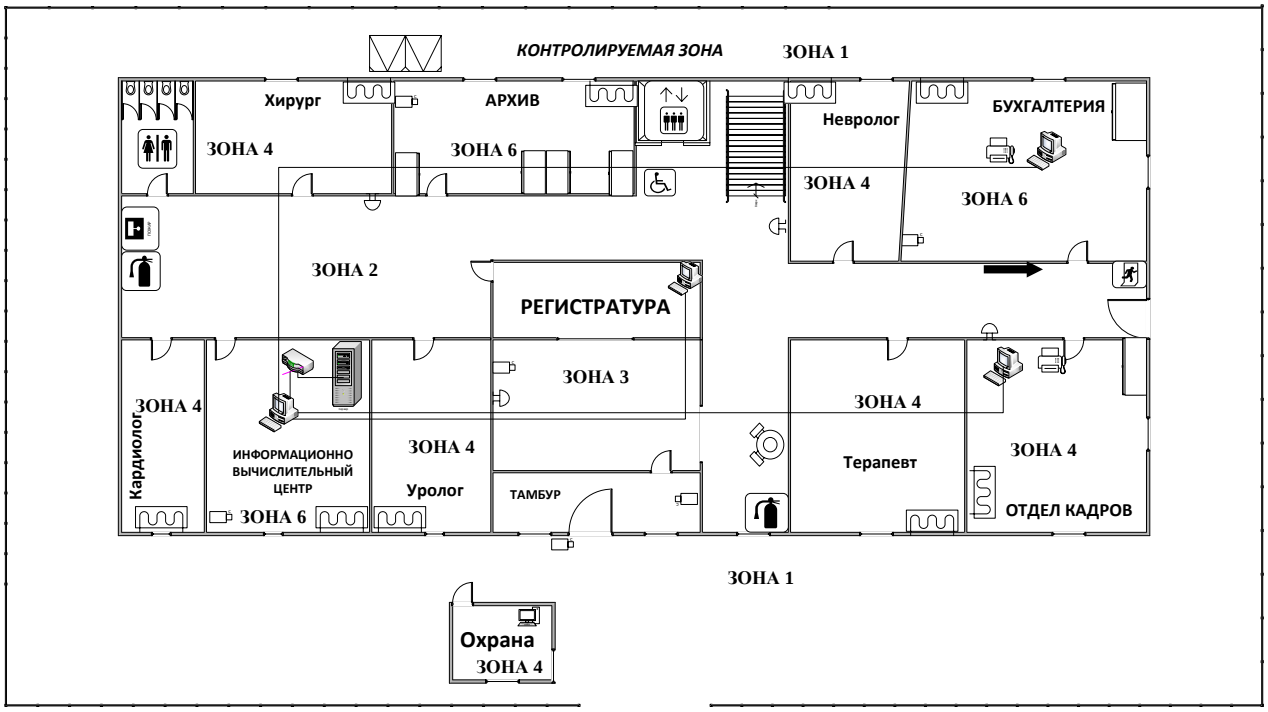


Рисунок 7.2 – Пример плана объекта защиты

На данном объекте показаны несколько зон системы безопасности, которые имеют структуру вложенных зон. В целях физической защиты объектов на базе построения зоны безопасности предприятия имеется система доступа и управления, которая также позволяет минимизировать возможность возникновения угроз. Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к различным составляющим объекта путем разделения его пространства на контролируемые зоны.

Определить категории контролируемых зон, заполнить таблицу 7.2 по данным исследуемого объекта защиты.

Таблица 7.2 – Описание контролируемых зон объекта по уровню доступа

Категория	Наименование зоны	Функциональное назначение зоны объекта	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны
I	Свободная	Заполнить по данному объекту	Свободный	Свободный	Есть
II	Наблюдаемая	Заполнить	Свободный	Свободный	Есть
III	Регистрационная	Заполнить	Свободный	Свободный с регистрацией по удостоверениям личности	Есть
IV	Режимная	Заполнить	По служебн. удостоверениям или идентификационным картам	По разовым пропускам	Усиленная охрана
V	Усиленной защиты	Заполнить	По спецдокументам	По спецпропускам	Усиленная охрана
VI	Высшей защиты	Заполнить	По спецдокументам	По спецпропускам	Усиленная охрана

Задание 4. Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты. Проанализировать характеристики технической укрепленности объекта защиты, заполнить таблицу 7.3.

Таблица 7.3 – Характеристики технической укрепленности объекта защиты

Наименование параметра	Данные
1	2
Площадь, кв.м	
Высота потолка, м	
Толщина стен: наружных, внутренних, м	
Окна: количество, размер	

Продолжение таблицы 7.3

1	2
Двери: размер проема, тип замков	
Описание смежных помещений: сверху, сбоку слева, сбоку справа, снизу	
Система электропитания (освещение): тип светильников и их количество	
Система заземления	
Системы сигнализации	
Система вентиляции (тип)	
Наличие экранов на батареях	
Телефонные линии: городская сеть, тип розеток	

Построение пространственной модели объекта защиты. Провести анализ месторасположения объекта (в какой части города расположен объект), какие объекты находятся в ближайшем окружении. Составить пространственную модель объекта по примеру таблицы 7.4.

Таблица 7.4 - Пространственная модель контролируемых зон

Пространственная характеристика помещения	Функциональная, конструктивная и техническая характеристика помещения		
Этаж	2	Площадь, м^2	56
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
Двери, кол-во, одинарные, двойные	4 двери звукоизолирующие тяжелые	Куда выходят двери	Коридор, каб. №3, каб. №2, каб. №1
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.		

Задание 5. 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.

Структурирование производится путем классификации защищаемой информации в соответствии с функциями, задачами и дальнейшей привязкой элементов информации к их носителям.

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. Пример структурной модели приведен на рисунке 2.1.

Для структурирования информации в качестве исходных данных используется перечень сведений составляющих государственную, ведомственную, коммерческую, врачебную 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:

- наименование элемента информации,
- категория 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 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 показаны на примере таблицы 7.5.

Таблица 7.5 - Структурная модель защищаемой информации

Наименование элемента информации	Категория информации	Источник информации	Вид носителя информации	Место нахождения информации
Структура предприятия	Служебная тайна	Документация	Бумажные и электронные носители	Шкаф с документами, каб. 1,3,5. ПЭВМ в каб. 1,2.3
Личные данные сотрудников	Персональные данные	Личные карточки сотрудников, трудовые книжки, трудовые договоры	Бумажные и электронные носители	Шкаф с документами, каб. 1,3,5, ПЭВМ в каб. 1,2.3
Финансовые документы	Коммерческая тайна	Ведомости, приходно-расходные ордеры, счет-фактуры	Бумажные и электронные носители	Сейф с документами, каб., ПЭВМ каб.3
Приказы по организации	Служебная тайна	Документация	Бумажные и электронные носители	Шкаф , каб. 1,3,5. ПЭВМ в каб. 1,2.3

Задание 6. Определение категории защищаемого объекта. В результате выполнения задач были определены функционально-отраслевая принадлежность исследуемого объекта, виды и масштабы возможного ущерба в результате нарушения безопасности, категория важности защищаемой информации на объекте.

Кроме названных характеристик необходимо определить пожаро- и взрывоопасность данного объекта, что осуществляется в соответствии с Федеральным законом № 117-ФЗ от 10 июля 2012 г. «Технический регламент о требованиях пожарной безопасности».

Результаты решения поставленной задачи занести в таблицу 7.6.

Таблица 7.6 – Категорирование исследуемого объекта защиты

Информативный признак категории	Категория исследуемого объекта
По функционально-отраслевой принадлежности	Заполнить в соответствии с данными объекта защиты
По виду возможного ущерба	Заполнить в соответствии с данными объекта защиты
По масштабу возможного ущерба	Заполнить в соответствии с данными объекта защиты
По важности объекта	Заполнить в соответствии с данными объекта защиты
По категория информации	Заполнить в соответствии с данными объекта защиты
По пожаро- и взрывоопасности	Заполнить в соответствии с данными объекта защиты
По численности персонала свыше 500 человек	Заполнить в соответствии с данными объекта защиты
По материальным активам свыше 500 МРОТ	Заполнить в соответствии с данными объекта защиты

Варианты объектов физической защиты

В таблице 7.7 представлены варианты объектов информатизации, для которых необходимо провести анализ защищаемой информации, угроз, разработать модель системы физической защиты в соответствии с заданиями практических работ.

Таблица 7.7 - Варианты объектов защиты

№ варианта	Объект информатизации
1	Здание администрации завода железобетонных изделий
2	Здание торгового центра
3	Здание поликлиники
4	Корпус университета
5	Здание научно-производственного объединения
6	Здание фармацевтической фирмы
7	Здание районного отдела полиции
8	Здание банка
9	Здание патентного бюро
10	Здание редакции научного издания
11	Здание научно-исследовательского института
12	Здание склада текстильной продукции
13	Здание рекламного агентства
14	Здание производственных цехов бурового оборудования
15	Здание птицефабрики
16	Здание республиканской библиотеки
17	Здание музея изобразительных искусств
18	Здание школы
19	Здание больницы
20	Здание районного суда

Контрольные вопросы

1 Дать определение системы физической защиты объекта информатизации. Пояснить цель и основные задачи физической защиты объектов информатизации.

2 Назвать и дать характеристику структуры и состава системы физической защиты объекта.

3 Назвать и охарактеризовать инженерно-технические средства защиты объектов информатизации.

4 Назовите основные организационные мероприятия физической защиты.

5 Назвать и дать определение принципов физической защиты.

6 В чем заключается принцип многозональности, назвать и пояснить виды контролируемых зон по структурной организации.

7 Назвать и дать характеристику всех возможных категорий контролируемых зон по условиям доступа.

8 В чем заключается принципы многорубежности, непрерывности, адаптируемости системы физической защиты?

9 Назвать и дать характеристику методов физической защиты объектов информатизации.

10 Назвать и пояснить этапы анализа объекта физической защиты.

11 По каким признакам проводится категорирование исследуемого объекта защиты. дать характеристику категорий по функционально-отраслевой принадлежности, по виду и масштабу ущерба.

12 Каким образом проводится категорирование объектов защиты по важности и по секретности информации? Назвать руководящие документы.

13 Назвать и дать характеристику категории защищаемых объектов по пожаро- и взрывоопасности.

14 Что представляет собой структурная модель защищаемой информации?

7.2 Практическая работа № 2. Анализ нормативно-правовой базы физической защиты. Формирование требований к физической защите объекта

Цель. Формирование требований к физической защите на основе анализа нормативно-правовых документов и характеристики объекта.

Задачи.

1 Изучить нормативно-правовые документы по физической защите объектов. Сформировать таблицу внешних и внутренних документов.

2 Сформировать перечень требований к системе физической защиты заданного объекта.

3 Определить количество рубежей защиты для заданного объекта, построить схему рубежей с пояснениями.

Задание 1. Изучить нормативно-правовые документы по физической защите объектов. Сформировать таблицу внешних и внутренних документов. Для заданного объекта в результате выполнения практической работы № 1 были выявлены такие характеристики, как категория важности объекта, категории защищаемой информации, категория объекта по взрыво- и пожароопасности, по виду и масштабу ущерба. Для реализации эффективной физической защиты объекта необходимо сформировать требования, которые предъявляют нормативно-правовые документы к объекту полученной категории.

Все нормативно-правовые документы можно разделить на 2 группы: руководящие документы федерального значения и отраслевые или внутренние документы, разработанные непосредственно для заданного объекта.

Построить таблицу по примеру таблицы 7.8.

Таблица 7.8 - Перечень нормативно-правовых документов физической защиты

Уровень документа	Наименование документа	Краткое пояснение
1	2	3
Федеральные	РД 25.952-90 Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации.	Устанавливает содержание и единый порядок разработки, согласования и утверждения здания на проектирование систем пожаротушения и сигнализации.
Федеральные	РД 78.147-93 Единые требования по технической укрепленности и оборудованию сигнализацией охраняемых объектов.	Устанавливают порядок и способы оснащения средствами механической защиты и охранной сигнализацией объектов различных форм собственности с целью противодействия преступным посягательствам на них.
Внутренние	Регламентация доступа в служебные помещения ГАУЗ «ГКБ №6» г. Оренбург	Во время обработки информации ограниченного распространения в таких помещениях должен присутствовать только персонал, допущенный к работе с данной информацией
	Инструкция по действиям персонала ГАУЗ «ГКБ №6» при возникновении чрезвычайных ситуаций	Определяет действия работников в случае возникновения на территории больницы и за ее пределами чрезвычайных ситуаций природного и техногенного характера, а также других ситуаций, которые могут создавать угрозу их жизни и здоровья
	Политика информационной безопасности ГАУЗ «ГКБ №6»	Регулируют управление, защиту и распределение ценной информации

Задание 2. Сформировать перечень требований к системе физической защиты заданного объекта. В соответствии с полученными данными обследования объекта составить таблицы требований к физическим средствам защиты заданного объекта информатизации в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств» по следующим пунктам:

- количество рубежей защиты объекта;
- класс защиты конструктивных элементов (строительные конструкции, дверные, оконные конструкции);
- класс защиты основного ограждения;
- класс защиты ворот;
- характеристики дверных конструкций;
- класс защиты запирающих устройств;
- типы извещателей для обнаружения криминального воздействия;
- наличие системы контроля доступа;
- характеристики системы видеонаблюдения;
- характеристики системы охранного освещения;
- характеристики системы оповещения.

Например, исследуемый объект относится к группе БІ:

- объекты с хранением или размещением изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и другого имущества;
- объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски и другие аналогичные объекты).

Пример требований к физической защите объекта указаны в таблице 7.9

Таблица 7.9 – Классы защиты и требования к элементам защиты

Элемент объекта	Класс защиты	Характеристика
1	2	3
Количество рубежей защиты	1	деревянные входные двери, погрузочно-разгрузочные люки, ворота - на открывание" и "разрушение" , остекленные конструкции - на "открывание" и "разрушение" стекла; металлические двери, ворота
Наружные стены здания первого этажа, также стены, перекрытия охраняемых помещений, расположенных внутри здания	1	Минимально необходимая степень защиты объекта от проникновения: гипсолитовые, гипсобетонные толщиной не менее 75 мм; щитовые деревянные конструкции толщиной не менее 45 мм
Ворота	1	Ворота 1 класса защиты (минимально необходимая степень защиты объекта от проникновения) - ворота из некапитальных конструкций высотой не менее 2 м.
Входные двери в здание, выходящие на оживленные улицы и магистрали	2	двери с полотнами из стекла в металлических рамах или без них
Внутренние двери в помещениях в пределах	1	двери деревянные внутренние со сплошным или мелкопустотным заполнением полотен по ГОСТ 6629-88, ГОСТ 14624-84, ГОСТ 24698-81. Толщина полотна менее 40 мм; двери деревянные со стеклянными фрагментами из листового обычного марок М4-М8 по ГОСТ 111-90, армированного по ГОСТ 7481-78, узорчатого по ГОСТ 5533-86, тонированного
Оконные проемы первого и подвального этажей	1	минимально необходимая степень защиты объекта от проникновения) - окна с обычным стеклом (стекло марки М4-М8 по ГОСТ 111-90, толщиной от 2,5 до 8 мм

Продолжение таблицы 7.9

1	2	3
Ограждение основное	1	Ограждения 1 класса защиты (минимально необходимая степень защиты объекта от проникновения) - ограждения из различных некапитальных конструкций высотой не менее 2 м.
Запирающие устройства внутренних дверей	1	Врезные и накладные замки: 1 класса по ГОСТ 5089-97; сувальдные. Не менее 6 сувальд для врезного замка или 5 - накладного; штифтовые.

По образцу таблицы 7.9 составить перечень требований к элементам физической защиты заданного объекта.

Задание 3. Определить количество рубежей защиты для заданного объекта, построить схему рубежей с пояснениями. Пример построения рубежей приведен на рисунке 7.3.

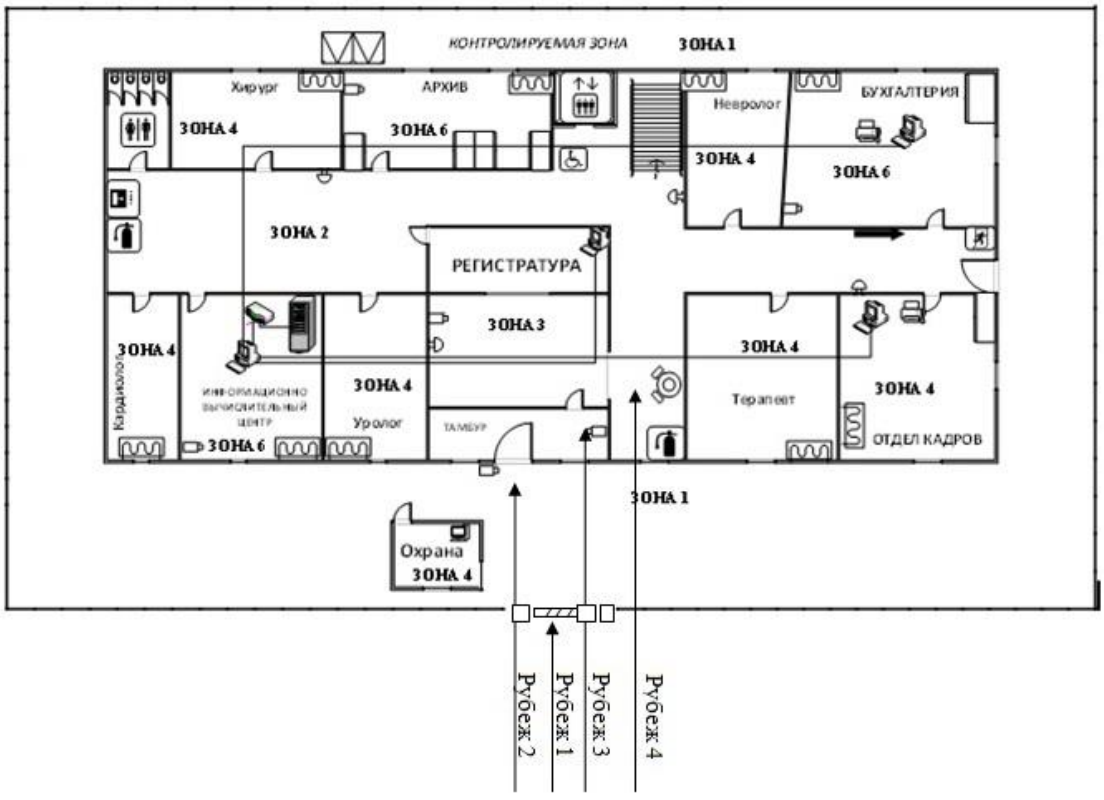


Рисунок 7.3 – Схема рубежей охраны

Контрольные вопросы.

1 Назовите основные нормативно-правовые документы, используемые при проектировании систем физической защиты.

2 Дать определение понятия «категория охраняемого объекта». В каком нормативном документе дано это определение.

3 Что подразумевается под инженерно-технической укрепленностью объекта? Какие элементы физической защиты характеризуют техническую укрепленность объекта?

4 Назовите объекты, которые относятся к особо важным, группы А I?

5 Назовите объекты, которые относятся к подгруппе А II?

6 Назовите объекты, которые относятся к подгруппе Б I, Б II?

7 По каким признакам классифицируются объекты, не вошедшие в перечни?

8 Дать определение понятия «класс защиты» конструктивных элементов физической защиты. Какой нормативный документ устанавливает соответствие класса защиты и категории объектов?

9 Что такое рубеж защиты? Каким образом определяется их количество? Дать характеристику рубежей защиты.

10Для какой цели организуется многорубежная защита и в каких случаях?

11 Какие параметры отличают ворота разных классов защиты?

12 Какие параметры характеризуют оконные конструкции?

13 Назовите параметры, характеризующие дверные конструкции. Приведите способы усиления дверных конструкций.

14 Дать определение понятий «равнопрочность рубежа защиты», «непрерывность защиты физической защиты», «надежность защиты».

7.3 Практическая работа № 3. Анализ источников угроз и путей проникновения нарушителя

Цель. Формирование перечня источников угроз и каналов утечки информации на защищаемом объекте.

Задачи.

1 Дать характеристику объектов воздействия и источников угроз физической безопасности.

2 Проанализировать уязвимости объекта.

3 Дать характеристику каналов утечки информации.

4 Построить схему путей проникновения нарушителя на объект.

Задание 1. Характеристика объектов воздействия источников угроз физической безопасности. Самый общий перечень угроз физической безопасности включает:

- диверсии;
- терроризм;
- негативное воздействие на технологические процессы;
- кража материальных и финансовых ценностей;
- кража и воздействия на информацию и ее носители;
- воздействия стихийных сил.

Все эти угрозы направлены на объекты угроз. Составить список объектов, подлежащих защите, оценить вид и масштаба ущерба с помощью вербальных показателей, и занести их в таблицу 7.10.

Таблица 7.10 – Объекты защиты, виды ущерба

Объекты защиты	Вид ущерба	Уровень ущерба
1	2	3
персонал	Физический, моральный, экономический	высокий

Продолжение таблицы 7.10

1	2	3
технологические процессы	Материальный, экономический	высокий
оборудование	Материальный, экономический	средний
готовая продукция	Материальный, экономический	высокий
интеллектуальная собственность	Экономический	высокий
средства вычислительной техники	Материальный, экономический	средний
Конфиденциальная информация	Потеря репутации компании, материальный, экономический	высокий
Заполнить по данным защищаемого объекта	Заполнить по данным защищаемого объекта	Заполнить по данным защищаемого объекта

Проанализировать виды источников угроз, сформировать перечень источников угроз и занести их в таблицу 7.11.

Таблица 7.11 – Виды источников угроз безопасности

Вид источника угроз		Перечень источников угроз
Техногенные	внешние	Средства связи, сети электропитания
		Системы кондиционирования
		Технические средства обработки информации
		Сети инженерных коммуникаций
		Заполнить по объекту
	внутренние	Неправильная конфигурация средств защиты
		Сбои в работе СКУД
		Заполнить по объекту
Антропогенные	Внешние нарушители	Заполнить по объекту
	Внутренние нарушители	Заполнить по объекту
Стихийные		Заполнить по объекту

Задание 2. Проанализировать уязвимости объекта.

Анализ уязвимости - совокупность действий, направленных на выявление уязвимых мест физической защиты объекта. Фактор, влияющий на уязвимость (фактор уязвимости) - признак наличия уязвимого места в физической защите.

Уязвимые места - элементы физической защиты, преодолевая которые нарушитель имеет наибольшую вероятность совершения диверсии или хищения ценных ресурсов предприятия. Все уязвимости можно разбить по их принадлежности к определенным подсистемам системы физической защиты. Сформулировать факторы уязвимостей защищаемого объекта по примеру таблицы 7.12.

Таблица 7.12 – Факторы уязвимостей защищаемого объекта

Уязвимости подсистем	Факторы уязвимости
1	2
Уязвимости подсистемы обнаружения	Входы (выходы) в зданиях, сооружениях и помещениях, расположенных во внутренней и особо важной зонах, не оборудованы техническими средствами обнаружения, средствами оптико-электронного наблюдения и управления доступом.
	Не обеспечено автоматическое переключение электропитания ТСФЗ на резервные источники при отключении основной системы.
	Отсутствует автоматический дистанционный контроль работоспособности ТСФЗ.
	Система оптико-электронного наблюдения не имеет подсистему видеозаписи и ее сохранения.
	Заполнить
Уязвимости подсистемы задержки	Входы (выходы) в зданиях, сооружениях и помещениях, расположенных во внутренней и особо важной зонах, не оборудованы замковыми устройствами, техническими средствами обнаружения, средствами оптико-электронного наблюдения и управления доступом.
	Физические барьеры, замедляющие проникновение нарушителя в охраняемую зону, находятся не на всех участках охраняемой зоны.
	Проемы, окна, вентиляционные короба, технологические проходы не обеспечены физическими барьерами.
	Заполнить

Продолжение таблицы 7.12

1	2
Уязвимости действий подразделений охраны	Время реагирования подразделений охраны не обеспечивает перехват нарушителя на возможных маршрутах следования нарушителя.
	Не соответствуют ведомственным нормативным документам по организации охраны ОИАЭ и порядку несения службы подразделениями охраны следующие характеристики подразделений охраны: − укомплектованность личным составом, − обеспеченность вооружением, транспортом и средствами связи, − профессиональная подготовка, прохождение периодической аттестации.
	Заполнить
Уязвимости подсистемы организационных мероприятий	Не соответствуют объему и характеру предъявляемых требований следующие организационно-распорядительные документы: − положение о службе безопасности, − положение о пропускном режиме и разрешительной системе допуска и доступа, − план охраны. Не установлен порядок выдачи и хранения ключей от охраняемых помещений.
	Заполнить

Задание 3. Дать характеристику 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, др.).

Провести анализ потенциальных каналов утечки на заданном объекте.

Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу таблицы 7.13.

Таблица 7.13 - Перечень потенциальных каналов утечки информации

Каналы утечки информации с объекта защиты		Место расположения
Оптический канал	Окна со стороны проспекта	каб. №1
	Окна, выходящие на улицу	каб. №2
	Окна, выходящие во внутренний двор	каб. №3
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
Акустический канал	Теплопровод подземный	указать
	Водопровод подземный	указать
	Стены помещения	указать
	Батареи	указать
	Окна контролируемого помещения	указать
Материально-вещественный канал	Документы на бумажных носителях	указать
	Персонал предприятия	указать
	Производственные отходы	указать

Задание 4. Построить схему путей проникновения нарушителя на объект. Несанкционированное проникновение на объект осуществляется в основном через окна, двери, балконы; на периметр - через проходную, лазы в заборе и непосредственно через ограду. Проанализировать возможные пути проникновения нарушителя и обозначить их на плане защищаемого объекта. Образец схемы проникновения представлен на рисунке 7.4.

Рисунок 7.4 – Пути проникновения нарушителя на объект

Контрольные вопросы.

1 Дать определение понятия «источник угроз безопасности». На какие классы подразделяются все источники угроз безопасности?

2 Охарактеризовать антропогенные источники угроз безопасности. Привести перечень возможных внешних и внутренних нарушителей.

3 Дать характеристику внутренних и внешних техногенных источников угроз безопасности.

4 Дать определение понятий «уязвимость физической защиты», «фактор уязвимости». Кратко пояснить, как определяются уязвимости физической защиты.

5 Назовите типичные уязвимости подсистемы организационных мероприятий.

6 Дать определение технического канала утечки информации, назвать типы каналов утечки.

7 Какие сведения включает пространственная модель каналов утечки?

7.4 Практическая работа №4. Построение модели нарушителя и модели угроз безопасности

Цель. Создание полной характеристики потенциального нарушителя безопасности и перечня актуальных угроз безопасности для заданного объекта.

Задачи.

1 Построение модели вероятного нарушителя безопасности объекта.

2 Разработка модели угроз безопасности объекта.

Задание 1. Построение модели вероятного нарушителя безопасности объекта. 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.

Составить список внешних и внутренних нарушителей безопасности заданного объекта. Проанализировать следующие характеристики, присущие нарушителям, заполнить таблицу 7.14.

Таблица 7.14 – Характеристики нарушителя

Признак характеристики нарушителя	Характеристика
1	2
Цели и задачи	проникновение на охраняемый объект без причинения объекту видимого ущерба
	причинение ущерба объекту
	преднамеренное проникновение при отсутствии враждебных намерений
	случайное проникновение
	Дополнить
Степень принадлежности вероятного нарушителя к объекту	сотрудник охраны
	сотрудник учреждения
	посетитель
	постороннее лицо
	Дополнить

Продолжение таблицы 7.14

1	2
Степень осведомленности вероятного нарушителя об объекте	детальное знание объекта
	осведомленность о назначении объекта, его внешних признаках и чертах
	неосведомленный вероятный нарушитель
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
Степень профессиональной подготовленности вероятного нарушителя	специальная подготовка по преодолению систем охраны
	не имеет специальной подготовки по преодолению систем охраны
Степень физической подготовленности вероятного нарушителя	специальная физическая подготовка
	низкая физическая подготовка
Владение вероятным нарушителем способами маскировки	владеет
	не владеет
Степень технической оснащенности вероятного нарушителя	высокая
	средняя
	низкая
Способ проникновения вероятного нарушителя на объект	взлом замка
	проход по поддельным документам
	Дополнить

Определить категорию нарушителя (существует четыре категории нарушителей).

Построить неформализованную модель нарушителя безопасности в соответствии с таблицей 3.1 данного учебного пособия.

Задание 2. Разработка модели угроз безопасности объекта. Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;

- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

Составить список всех возможных угроз физической безопасности для заданного объекта. При этом использовать перечень угроз, данный в таблице 3.3 учебного пособия. Вычислить все необходимые показатели угроз. Построить модель угроз по примеру таблицы 7.15.

Таблица 7.15 - Модель угроз безопасности защищаемого объекта

Угроза	Вероятность реализации угрозы	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Несанкционированный доступ к компьютерам	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража технических средств с хранящейся в них информацией	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража носителей информации	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража материальных и финансовых ценностей	Средняя вероятность (5)	0,5 (средняя)	Высокая	Актуальная
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероятность (5)	0, 6 (средняя)	Высокая	Актуальная
Прослушивание телефонных и радиопереговоров	Средняя вероятность(5)	0,5 (средняя)	Высокая	Актуальная
Внедрение «закладок»	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная

Выписать из таблицы только актуальные угрозы безопасности.

Контрольные вопросы

1 Дать определение понятия «угроза физической безопасности», «нарушитель физической безопасности».

2 Назвать и дать характеристику типичных угроз физической безопасности объектов информатизации.

3 Назвать типичные объекты воздействия угроз безопасности.

4 Назвать и охарактеризовать типы и категории нарушителей.

5 Какой тип нарушителя считается самым опасным, привести обоснование ответа.

6 Дать определение понятия «модель нарушителя». Назвать и описать основные характеристики нарушителя безопасности.

7 Дать определение понятия «формализованная модель нарушителя». Привести методы построения формализованной модели нарушителя.

8 Перечислить основные действия, которые может совершить внешний нарушитель.

9 Дать определение понятия «модель угроз безопасности». Назвать основные показатели, определяющие актуальность угроз.

10Что подразумевают под частотой (вероятностью) реализации угрозы? Назовите вербальные градации этого показателя.

11 За счет чего могут быть реализованы угрозы безопасности.

12 По какой формуле определяется коэффициент реализуемости угрозы, какова вербальная интерпретация реализуемости угрозы?

13 Каким образом оценивается опасность каждой угрозы?

14 Как используют в дальнейшем список актуальных угроз безопасности?

7.5 Практическая работа № 5. Выбор и обоснование средств подсистемы задержки

Цель. Формирование подсистемы задержки нарушителя безопасности

Задачи.

1 Определение количества и типа рубежей физической защиты.

2 Выбор и обоснование основного ограждения.

3 Выбор и обоснование ворот и дверных конструкций.

4 Выбор и обоснование запорных устройств.

5 Выбор и обоснование оконных конструкций

6 Выбор и обоснование шкафов и сейфов.

Задание 1. Определение количества и типа рубежей физической защиты. В практической работе № 2 была определена категория объекта и сформулированы основные требования по технической укрепленности обьекта защиты. В соответствии с этими требованиями должно быть определено количество рубежей защиты и класс защиты средств технической укрепленности объекта.

Привести сведения о категории объекта и соответствующих ей классах защиты средств задержки в таблице 7.16.

Таблица 7.16 – Сведения о классах защиты средств подсистемы задержки

Наименование средства задержки	Класс защиты
Количество рубежей защиты	Указать
Основное ограждение	Указать
Ворота, калитки	Указать
Наличие шлагбаума	Указать
Оконные конструкции	Указать
Дверные конструкции	Указать
Запорные устройства	Указать
Наличие КПП	Указать
Сейфы	Указать
Шкафы	Указать

Задание 2. Выбор и обоснование основного ограждения. Провести выбор и обоснование основного ограждения. Привести характеристики основного ограждения в таблице 7.17.

Таблица 7.17- Характеристика основного ограждения

Наименование	Характеристика
Высота ограждения	Заполнить
Просматриваемость ограждения	Заполнить
Деформируемость ограждения	Заполнить
Вид полотна ограждения ограждения	Заполнить
Материал опор ограждения	Заполнить
Материал фундамента ограждения	Заполнить
Тип установки ограждения	Заполнить
Вид ограждения	Заполнить

Задание 3. Выбор и обоснование ворот и дверных конструкций. Провести выбор и обоснование ворот и дверных конструкций. Привести характеристики в таблице 7.18.

Таблица 7.18- Характеристика ворот и дверных конструкций

Наименование	Характеристика
Материал дверей	Заполнить
Прочность	Заполнить
Пулестойкость	Заполнить
Способ открытия (наружу или внутрь)	Заполнить
Толщина дверей	Заполнить

Задание 4. Выбор и обоснование запорных устройств. Провести выбор и обоснование запорных устройств. Привести характеристики в таблице 7.19.

Таблица 7.19- Характеристика запорных устройств

Наименование	Характеристика
Вид замка на воротах	Заполнить
Взломоустойчивость	Заполнить
Вид замка входной двери	Заполнить
Вид замка внутренних дверей	Заполнить

Задание 5. Выбор и обоснование оконных конструкций. Провести выбор и обоснование оконных конструкций. Привести характеристики в таблице 7.20.

Таблица 7.20- Характеристика оконных конструкций

Наименование	Характеристика
Защитные решетки, Жалюзи	Заполнить
Тип и толщина стекла	Заполнить
Материал оконных рам	Заполнить

Задание 6. Выбор и обоснование шкафов и сейфов. Провести выбор и обоснование шкафов для хранения секретных документов и сейфов для хранения ценных документов и денежных средств. Привести характеристики в таблице 7.21.

Таблица 7.21- Характеристика шкафов и сейфов

Наименование	Характеристика
Материал шкафа	Заполнить
Толщина стенок шкафа	Заполнить
Вид замка шкафа	Заполнить
Материал сейфа	Заполнить
Вес сейфа	Заполнить
Вид замка сейфа	Заполнить

Контрольные вопросы.

1 Что такое рубеж охраны? Дать определение однорубежной и многорубежной систем. Привести примеры.

2 Какие факторы и каким образом оказывают влияние на выбор средств подсистемы задержки?

3 Дать характеристику средств инженерно-технической укрепленности объекта.

4 Назовите все типы основного ограждения и поясните их конструкцию.

5 В каких случаях применяют сигнализационное заграждение? Для каких объектов применяют электризуемое ограждение?

6 Что такое зона отторжения? Назовите основные задачи этой зоны? Какие технические средства в ней размещают?

7 Ограждения с какими характеристиками применяют для защиты объектов категории AI?

8 Какие технические средства применяют для защиты оконных систем? Какие средства применяют для обнаружения разбития стекла?

9 Перечислите все подсистемы охраны периметра и поясните их главные задачи.

10 Проведите анализ оконных конструкций с точки создания уязвимостей в системе физической защиты.

11 Какие параметры характеризуют надежность запирающих устройств?

12 Какие материалы используют для изготовления шкафов для хранения ценной документации? Какие дополнительные средства защиты ценной документации на бумажных носителях могут быть рекомендованы?

13 Какие материалы применяются для изготовления сейфов? Чем отличаются сейфы разных классов защиты?

14 Какие виды замков являются наиболее надежными? Назовите параметры, характеризующие надежность замков.

7.6 Практическая работа № 6. Выбор и обоснование средств подсистемы обнаружения нарушителя и признаков пожара

Цель. Формирование подсистемы обнаружения нарушителя безопасности

Задачи.

1 Провести выбор и обоснование охранных извещателей.

2 Провести выбор и обоснование пожарных извещателей.

3 Провести выбор средств оповещения.

4 Разработать схему размещения средств подсистемы обнаружения на объекте.

Задание 1. Провести выбор и обоснование охранных извещателей.

Периметр — внешняя граница (контур) защищаемой территории объекта, несанкционированное преодоление которого должно вызывать сигнал тревоги с указанием места его преодоления. Для эффективного решения задачи важно оптимальное сочетание механических преград, прежде всего пассивного ограждения (забора) периметра, с техническими средствами обнаружения (сигнализацией).

Главная задача любой системы охраны периметра — обеспечение максимальной вероятности обнаружения нарушителя с точным указанием места проникновения для организации эффективного противодействия.

При оснащении периметра средствами защиты необходимо учитывать факторы, влияющие на выбор подсистемы обнаружения. В России природные условия отличаются большим разнообразием. Большие сезонные колебания температуры, в некоторых районах доходящие до 80...90° С, сильные снегопады, метели, мокрый снег, гололед, иней, туманы, ураганные ветры, сильные дожди вызывают большие трудности при выборе соответствующего оборудования для защиты периметра. Кроме климатических факторов необходимо учитывать возможные источники помех, затрудняющих работу

охранных извещателей. Таковыми являются железнодорожные пути. Линии электропередач, радио- и телемачты и т.д.

Факторы, влияющие на выбор средств обнаружения, по вариантам указаны в таблице 7.22. Виды растительности: Н - низкая (кустарник), С – средняя (высокие кусты акации, сирени и т.д.), В – высокая (деревья).

Таблица 7.22 – Факторы, влияющие на выбор средств защиты по вариантам

№ варианта, фактор	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Наличие полосы отчуждения	+	_	_	_	_	_	_	_	_	_	_	+	_	_	+	_
Особенности рельефа местности	_	+	_	+	_	+	_	+	_	+	_	+	_	+	_	+
Наличие вблизи объекта ж/д	+	_	_	+	_	_	+	_	_	+	_	_	+	+	_	+
Наличие вблизи объекта линий электропередачи	_	+	+	_	+	+	_	+	+	_	+	+	_	_	+	_
Виды растительности	Н	Н	Н	С	С	В	С	В	Н	С	В	В	Н	Н	В	С
Трубопровод	_	+	_	_	_	_	+	_	+	_	_	+	_	_	_	+
Разрыв периметра для проезда транспорта, прохода людей	+	-	+	+	+	+	-	+	-	+	+	-	+	+	+	-

Выбор конкретного типа извещателя определяется в зависимости от:

— сопоставления конструктивных строительных характеристик объекта, подлежащего защите, и тактико-технических характеристик извещателя;

— характера и размещения ценностей в помещениях;

— помеховой обстановки на объекте;

— вероятных путей проникновения нарушителя;

— режима и тактики охраны.

Выбрать охранные извещатели, привести их характеристики и заполнить таблицу 7.23.

Таблица 7.23 – Спецификация охранных извещателей

Вид охранного извещателя	Функция	Модель извещателя	Место установки	Кол-во	Фирма изготовитель
Магнитоконтактные	Блоктровка дверей и окон	СМК-1	Двери	23	Специнформатика-СИ
Радиолучевой	Обнаружение пересечения периметра	Аргус-2	Ограждение	12	Аргус-Спектр
Акустический	Обнаружение разбития стекла	Стекло-3	Окна	26	Аргус-Спектр

Задание 2. Провести выбор и обоснование пожарных извещателей.

В зависимости от назначения здания, где устанавливается система пожарной безопасности, применяются и определенные датчики. Например, для установки пожарной сигнализации в складском помещении большого метража применяются лучевые датчики. Для установки пожарной сигнализации в помещениях с большим количеством находящихся в нем людей (кинотеатры, театры, библиотеки и др.) лучше всего использовать дымовые датчики. Если мы имеем дело со складским помещением, в котором хранится, например, древесина или другие легко воспламеняющиеся природные материалы, рекомендовано применять датчики, которые реагируют на открытый огонь.

Должны учитываться мельчайшие детали помещения, в котором происходит установка пожарной сигнализации. Поскольку тепловые датчики несколько инертны при срабатывании, предпочтительней использовать датчики дымовые. На рынке пожарного оборудования существуют также комбинированные датчики. Они предназначены для оповещения о пожаре при изменении двух параметров (температурном и дымовом).

Установка пожарной сигнализации позволяет не только оповестить людей о пожаре, но и вовремя локализовать возгорание и тем самым попутно избежать материальных потерь, что тоже немаловажно.

Провести выбор пожарных извещателей в соответствии с категорией объекта. Привести характеристики выбранных извещателей. Заполнить таблицу по образцу таблицы 7.24.

Таблица 7.24 – Спецификация пожарных извещателей

Вид пожарного извещателя	Функция	Модель извещателя	Место установки	Кол-во	Фирма изготови-тель
Дымовой оптикоэлектронный	Обнаружение дыма	ИП 212-64	Все помещения	23	Энерготрейд - системы
Газовый	Обнаружения газа	Указать модель	Каб. № 3,5,8	3	указать
Пламени	Обнаружение пламени	Указать модель	Каб. № 10,12	2	указать

Задание 3. Провести выбор средств оповещения. При определении типа системы оповещения и выборе оборудования для ее проектирования необходимо руководствоваться нормативными документами, утвержденными в установленном законом порядке. В первую очередь, это НПБ 77-98 (Нормы пожарной безопасности), устанавливающие общие технические требования к техническим средствам оповещения и управления эвакуацией, и НПБ 104-03, устанавливающие требования пожарной безопасности к СОУЭ, а также их типы с определением перечня объектов, подлежащих оснащению такими системами.

Требования настоящих норм при выборе оборудования и проектировании систем оповещения являются обязательными. Для большинства небольших и средних объектов нормами пожарной безопасности определена установка СОУЭ 1-го и 2-го типов.

Для заданного объекта выбрать средства пожарного оповещения с учетом конкретных условий на объекте. Привести техническое описание выбранных средств оповещения. Классификация, общие технические требования и методы испытаний охранных оповещателей указаны в ГОСТ Р 54126-2010. Для заданного объекта выбрать тип охранных оповещателей.

Привести характеристики выбранных средств оповещения. Заполнить таблицу по образцу таблицы 7.25.

Таблица 7.25 – Спецификация оповещателей

Вид оповещателя	Функция	Модель	Место установки	Кол-во	Фирма изготови-тель
Речевой	заполнить	заполнить	заполнить		заполнить
Звуковой	заполнить	заполнить	заполнить		заполнить
Световой	заполнить	заполнить	заполнить		заполнить

Задание 4. Разработать схему размещения средств подсистемы обнаружения на объекте. Пример схемы размещения средств подсистемы обнаружения приведен на рисунке 7.5.

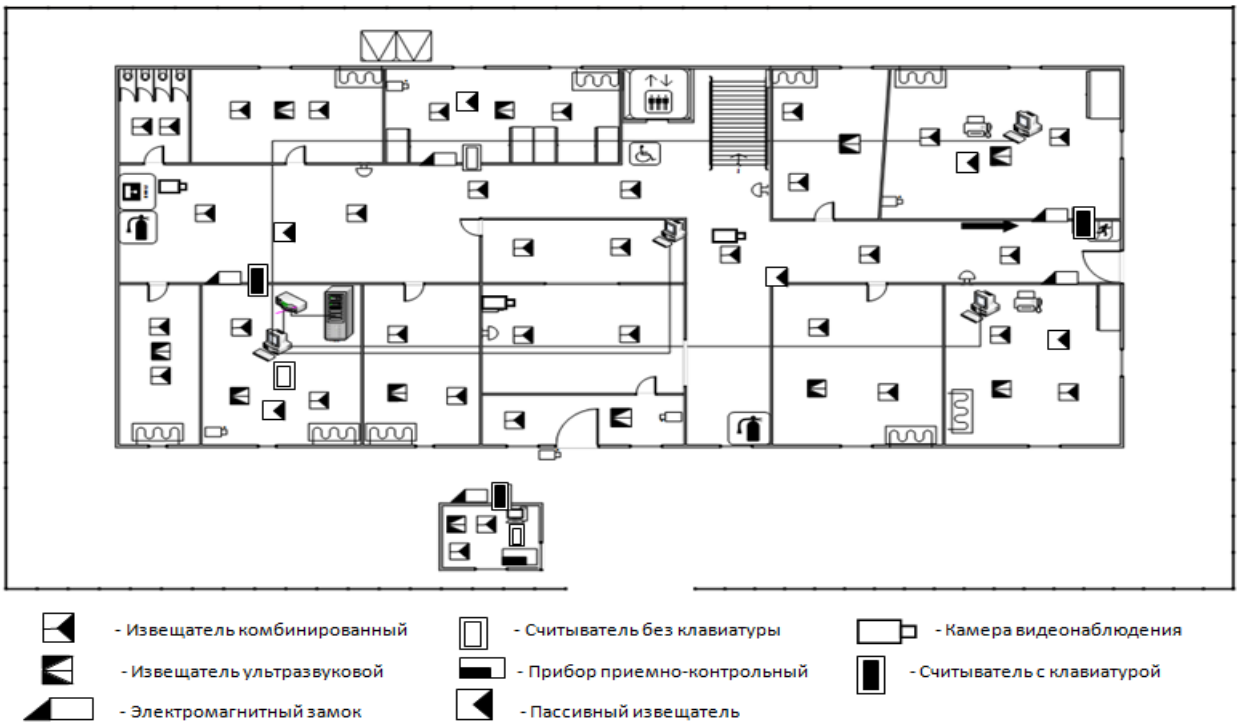


Рисунок 7.5 - Схема размещения средств подсистемы обнаружения

При разработке схемы расположения средств подсистемы обнаружения необходимо учитывать требования по геометрическим признакам помещений и территорий, а также технические характеристики приборов. Обозначения охранно-пожарного оборудования согласно требованиям рекомендаций РД 78.36.002-99 ГУВО МВД России. Технические средства систем безопасности объектов. Обозначения условные графические.

Контрольные вопросы.

1 Дать характеристику классов извещателей по назначению, принципам работы и виду зоны обнаружения.

2 Дать определение активных и пассивных технических средств обнаружения. Назвать типы активных извещателей.

3 Назвать типы контактных извещателей, охарактеризовать принципы работы магнитоконтактных извещателей.

4 Назвать типы акустических извещателей. Способы повышения помехоустойчивости ультразвуковых извещателей.

5 Назвать типы оптико-электронных извещателей. Принципы повышения помехоустойчивости пассивных и активных оптико-электронных извещателей.

6 Пояснить принципы работы пожарных извещателей.

7 Перечислить преимущества и недостатки тепловых извещателей.

8 Какие факторы учитываются при размещении охранно-пожарных извещателей на объекте?

9 Назовите преимущества емкостных извещателей. На каких объектах наиболее эффективно применять емкостные извещатели?

10 Какие извещатели используют для обнаружения движения в объеме?

11 Какие технические средства применяют для защиты оконных систем? Какие средства применяют для обнаружения разбития стекла?

12 В каких случаях целесообразно применение магнитоэлектрических извещателей?

7.7 Практическая работа № 7. Выбор и обоснование приемно-контрольного прибора

Цель. Ознакомление с приборами приемно-контрольными охранно-пожарными, построение спецификации оборудования.

Задачи.

1 Привести описание приемно-контрольного прибора по варианту, привести его структурную схему, сформулировать функции.

2 Представить технические характеристики ПКП, описать существующие режимы работы оборудования.

3 Представить и описать типовую схему применения прибора.

Варианты ПКП указаны в таблице 7.26.

Таблица 7.26 – Варианты заданий

№ варианта	Модель ПКП	№ варианта	Модель ПКП	№ варианта	Модель ПКП
1	Астра-812-М	6	Кодос А-20	11	Тандем -2М
2	Сигнал 20	7	Гранит-16/24	12	БШС8–И
3	Сигнал 10	8	Астра -713	13	Нота -2
4	С2000	9	Кварц	14	Астра-712/2
5	А16-512	10	Сигнал-ВК6	15	Гранит-12 USB

Задание 1. Привести описание приемно-контрольного прибора по варианту, привести его структурную схему, сформулировать функции.

Описание прибора должно включать следующие пункты:

- назначение прибора;
- область применения (перечень типов объектов);
- вид сети передачи данных (проводная, беспроводная);
- внешний вид прибора;
- описание принципа работы прибора.

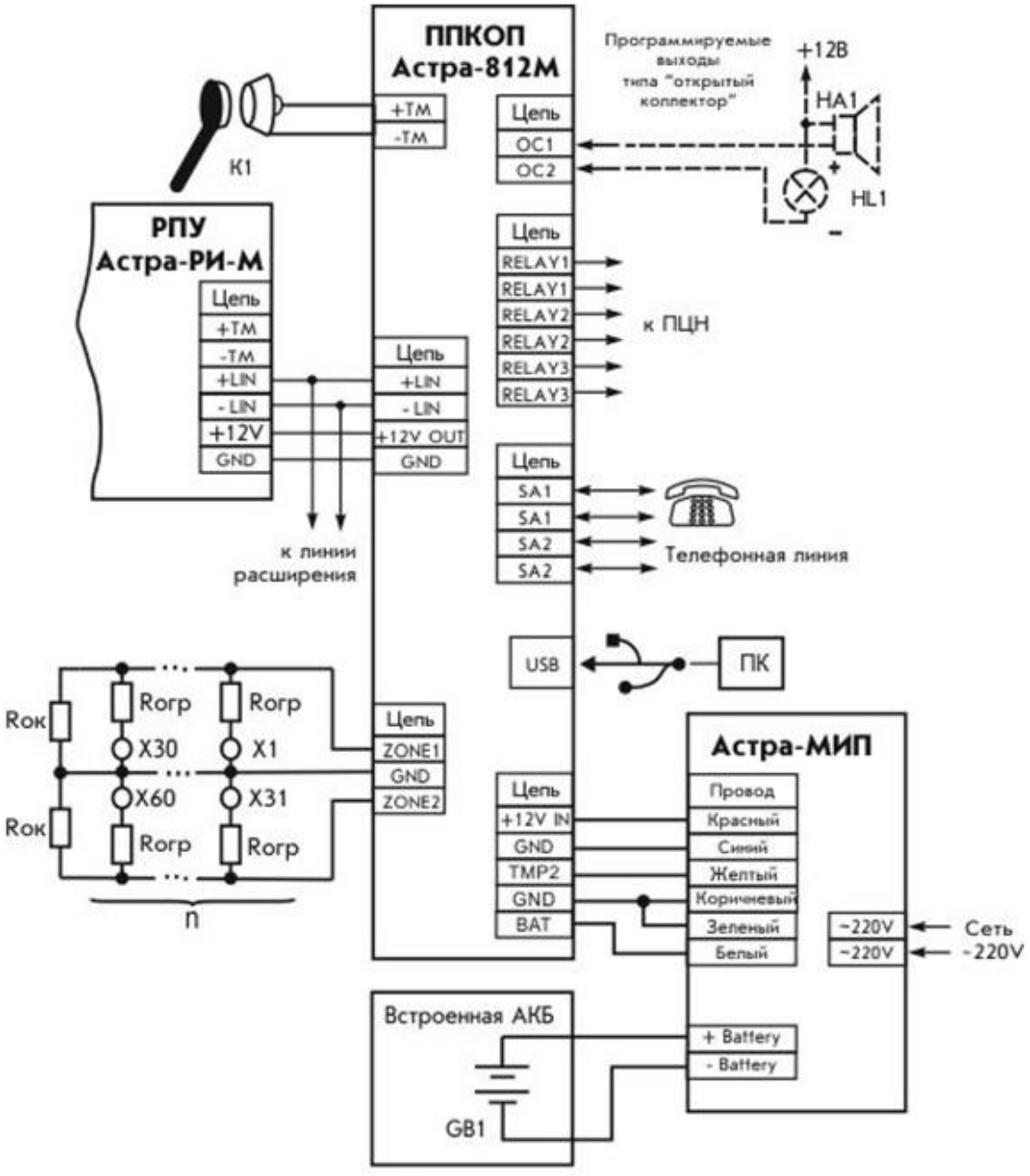
Задание 2. Представить технические характеристики ПКП.

Привести технические характеристики ПКП по примеру таблицы 7.27.

Таблица 7.27 — Основные технические характеристики прибора

Наименование параметра		Значение параметра
Количество радиальных неадресных шлейфов сигнализации (ШС)		20
Макс. сопротивление проводов ШС без учета оконечного сопротивления		1 кОм для охранных ШС 100 Ом для пожарных ШС
Допустимое сопротивление утечки между проводами ШС или каждым проводом и "землёй"		20 кОм для охранных ШС 50 кОм для пожарных ШС
Подключае-мые к ШС устройства	Неадресные охранные и пожарные извещатели с релейным выходом	Без ограничений
	Неадресные охранные извещатели, питающиеся от ШС	с общим током потребления до 3 мА
	Неадресные пожарные извещатели, питающиеся от ШС	с общим током потребления до 3 мА (с общим током потребления до 1,2 мА при одновременном включении тепловых и дымовых извещателей)
Световая индикация		1 индикатор отображения режимов
Встроенный звуковой сигнализатор		нет
Энергонезависимый буфер событий		62 сообщения
Интерфейс		RS-485, протокол Орион
Питание прибора		от внешнего источника постоянного тока
Напряжение питания		10,2 ÷ 28,0 В постоянного тока
Количество вводов питания		2
Готовность к работе после включения питания		не более 3 с
Рабочий диапазон температур		от -30 до +50 °С
Степень защиты корпуса		IP20
Средний срок службы		10 лет
Программирование прибора		программа UProg.exe
Подключение к ПК		через интерфейс RS-485

Задание 3. Представить и описать типовую схему применения прибора. В качестве примера на рисунке 7.6 приведена Типовая схема применения прибора.



K1 - считыватель Touch memory;
HA1 - звуковой оповещатель;
HL1 - световой оповещатель;
X1...X240 - активный извещатель;
n - количество извещателей (не более 30);
Rогр - ограничивающий резистор;
Rок - оконечный резистор

Рисунок 7.6 - Типовая схема ПКП

Контрольные вопросы.

1 Дать определение прибора приемно-контрольного охранно-пожарного, пояснить его назначение.

2 Дать характеристику функций приемно-контрольного прибора.

3 Дать характеристику классов ПКП по виду организации тревожной сигнализации и способу контроля извещателей.

4 В чем отличие ПКП, предназначенных для адресных и пороговых ОПС?

5 Что такое информационная емкость ПКП, какие классы ПКП бывают по этому параметру.

6 Назовите основные технические характеристики ПКП.

7 Назвать все узлы, входящие в состав ПКП, пояснить их назначение.

8 Описать структурную схему и пояснить принцип работы ПКП.

9 Что такое шлейф сигнализации? Сколько шлейфов входит в один ПКП?

10 Назовите и опишите основные режимы работы ПКП.

11 Приведите примеры видов электропитания ПКП.

12 Каким образом осуществляется электропитание ПКП? От каких источников запитываются шлейфы, в случае сбоев электросети?

13 Что такое информативность ПКП, в чем она измеряется?

14 Назовите и поясните способы подключения звуковых и световых оповещателей к ПКП.

7.8 Практическая работа № 8. Разработка структурной схемы и спецификации оборудования

Цель. Построение структурной схемы физической защиты объекта.

Задачи.

1 Разработать структурную схему физической защиты объекта.

2 Составить полную спецификацию оборудования физической защиты объекта.

Задание 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.

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.

Пример структурной схемы физической защиты представлен на рисунке 7.7.

Рисунок 7.7 – Пример структурной схемы физической защиты объекта

Задание 2. Составить полную спецификацию оборудования физической защиты объекта. Пример спецификации оборудования приведен в таблице 7.28.

Таблица 7.28 - Спецификации оборудования

Наименование	Производитель	Количество	Примечание
1	2	3	4
СПД 3.3	НПФ «Полисервис»	61	Пожарный извещатель оптический комбинированный тепло-дымовой.
КХ-08	OPTEX CO LTD	10	Извещатель охранный объемный потолочного крепления. Датчик движения, пассивный.
Астра-642	НТЦ «ТЕКО»	22	Извещатель ультразвуковой, объемный, дальность 10м, невосприимчивость к тепловым помехам. Датчик разбития стекла.

Продолжение таблицы 7.28

1	2	3	4
Сигнал-20П (SMD)	«Болид»	1	Прибор приемно-контрольный охранно-пожарный на 20 шлейфов.
ST-CE010EM	«Smartec»	2	Считыватель настольный для ввода идентификаторов EM. Контроль доступа к серверу.
ST-SC141EHK	«Smartec»	5	Автономный вандалозащищенный контроллер со встроенными считывателем EM+HID
ML-194 K	«AccordTec»	6	Электромагнитный замок усилие не менее 500 кг с платой управления.
MDC-AH7290FTD-24S	«MicroDigital Inc»	4	Купольная AHD камера для помещений, 2.0 Megapixel.

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)?

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 Боровский, А.С. Идентификация предметной области проектирования и оценки систем физической защиты // Наука и образование транспорту. - № 1, - 2011. - С.74-76.

3 Боровский, А.С. Автоматизированное проектирование и оценка систем физической защиты потенциально опасных объектов. Системный анализ проблемы проектирования и оценки систем физической защиты: монография / А. С. Боровский, А. Д. Тарасов. – Самара: СамГУПС, 2012. – 155 с.

4 Бочков, А. Категорирование критически важных объектов по уязвимости к возможным противоправным действиям. Экспертный подход. /А.Бочков // Безопасность. Достоверность. Информация. - № 1, -2009.- С.22-24.

5 Бурькова Е.В. Прикладная программа оценки физической защищенности объекта на основе логико-вероятностного подхода / Е.В. Бурькова, Д.А. Гайфулина, Э.Р. Хакимова// Материалы VI Международной научн.-практ. конф.: Информационные ресурсы и системы в экономике, науке и образовании.- Пенза: Общество «Знание» России». - 2016 г. – С. 10-14.

6 Бурькова, Е.В. Категорирование объектов информатизации для выбора средств физической защиты / Е.В. Бурькова // Материалы Всероссийской научно-методической конференции «Университетский комплекс как региональный центр образования, науки и культуры». - Оренбургский гос. ун-т. – Оренбург: ООО ИПК «Университет», 2017. С.

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

8 Бурькова, Е.В. Некоторые аспекты оценки эффективности функционирования систем безопасности / Е.В. Бурькова // X Всерос. научн.-практ.

конф. «Современные информационные технологии в науке, образовании и практике». – Оренбург: ООО ИПК «Университет», 2012. – С. 153-156.

9 Вишняков, С. М. Системы комплексной безопасности, категории и уровни защищенности стационарных объектов. / С.М. Вишняков. //Системы безопасности. - №1. - 2004. – С.26-32.

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

11 Волхонский, В.В. Устройства охранной сигнализации / В.В. Волхонский. – СПб.: Экополис и культура, – 2000. – 312 с.

12 Ворона, В.А.Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - М.: Горячая линия – Телеком, 2012. - 512 с.

13 ГОСТ Р 54126-2010 Оповещатели охранные. Классификация. Общие технические требования и методы испытаний. – Введен 21.12.2010.- М.: Изд-во стандартов, 2010.- 27 с.

14 ГОСТ РД 78.36.003-2002 Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств. – Введен 01.01.2003.- М.: Изд-во стандартов, 2002.- 32 с.

15 ГОСТ Р 50776-95 Системы тревожной сигнализации. Введен 01.01.1996.- М.: Изд-во стандартов, 1996.- 24 с.

16 ГОСТ РД 51241-2008.Средства и системы контроля и управления доступом. Введен 01.09.2009.- М.: Изд-во стандартов, 2009.- 34 с.

17 Грибунин, В.Г. Комплексная система защиты информации на предприятии. / В.Г. Грибунин, В.В. Чудовский, - М.: Издательский центр «Академия», 2009. – 416 с.

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

19 Дураковский, А.П. Применение математического аппарата при проектировании систем физической защиты./ А.П. Дураковский, В.Р. Петров// Безопасность информационных технологий. – 2012, № 2. - С. 80-84.

20 Зайцев, А. Категорирование объектов. / А. Зайцев // Алгоритм безопасности. – 2006, № 6. - С.7-9.

21 Коновалов, В.А. Категорирование объектов. Ключевой фактор обеспечения эффективности систем комплексной безопасности. /В.А. Коновалов, Д.В. Севрюков, Р.С. Хасянов. [Электронный ресурс].– Режим доступа:http://www.secuteck.ru/articles2/kompleks_sys_sec/kategorirovanieobiektov

22 Костин, В.Н. Методика формирования требований к системе физической защиты на основе концептуальной имитационной модели/ В.Н. Костин, С.Н. Шевченко // Инфокоммуникационные технологии. – 2013, № 2 – С.91-98.

23 Костин, В.Н. Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем: монография / В.Н. Костин, С.Н. Шевченко, Н.В. Гарнова. – Оренбург: ООО ИПК «Университет», 2014. – 202 с.

24 Лукоянов, С.В., Основные требования к системам физической защиты на этапе их проектирования. / С.В. Лукоянов, С.В. Белов // Вестник астраханского государственного технического университета. – 2010, № 2 – С. 163-171.

25 Магуенов, Р.Г. Охранная сигнализация и другие элементы систем физической защиты. Краткий толковый словарь./ Р.Г. Магуенов. – М.: Горячая линия – Телеком, 2007. – 97 с.

26 Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования. Свод правил. СП 132.13330.2011.

27 Панин, О. Категорирование объектов для создания эффективных систем физической защиты./ О. Панин // Безопасность. Достоверность. Информация. - № 70. – 2007. - С. 20-24.

28 Панин, О. Проблемы оценки эффективности функционирования систем физической защиты объектов. / О. Панин // Безопасность.

Достоверность. Информация. - № 3. – 2007. - С. 22-27.

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

30 Петров, Н.В. Системы физической защиты. Модульное проектирования и оценка эффективности. / Н.В. Петров // Защита информации. INSIDE. – 2009, № 5. - С. 55- 59.

31 Пожидаев, В.А. Пути повышения обоснованности требований к системам физической защиты объектов экономики на основе их категорирования по уровню значимости и риску диверсионно-террористического воздействия / В.А. Пожидаев, С.И. Припадчев // Вопросы защиты информации. – 2007, № 3. – С. 13-17.

32 Рытов, М.Ю. Модель процесса выбора состава технических средств систем физической защиты. / М.Ю. Рытов, В.Т. Еременко, М.Л. Гулак // Информация и безопасность.- 2015, № 4. - С. 502-507.

33 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.

34 Синилов В. Г. Системы охранной, пожарной и пожарно-охранной сигнализации: учебник для нач. проф. образования / В. Г. Синилов. 6-е изд. — М. : Издательский центр «Академия», 2011. — 512 с.

35 Системы и комплексы охранной сигнализации. Элементы технической укрепленности РД 78.143-92.

36 Системы автоматического пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Обозначения условные графические элементов систем РД 25.953-90.

37 Стрельцов, А.А. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова. – М.: Издательский центр «Академия», 2008. - 256 с.

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

Учебное пособие

Елена Владимировна Бурькова

ФИЗИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

ISBN 978-5-7410-1697-8