Фе­­­деральное агентство связи

Государственное бюджетное образовательное учреждение

высшего профессионального образования

Ордена Трудового Красного Знамени

Московский технический университет связи и информатики

Факультет информационных технологий

Кафедра «Информатика»

Курсовая работа

по дисциплине «Основы программирования»

Тема: «Физическая защита объектов информатизации»

Выполнил: студент

группы БСТ-2001

Бессолицын А.Д.

Руководитель: доцент

кафедры «Информатика»

Гуриков С.Р.

Москва, 2020

**Оглавление**

[**Введение** 3](#_Toc54900859)

[**Техническое задание** 5](#_Toc54900860)

[**Глава I. Теоретическая часть** 7](#_Toc54900861)

[**1.1 Сущность и задачи физической защиты объектов информатизации** 7](#_Toc54900862)

[**1.1.1 Анализ структуры физической защиты** 7](#_Toc54900863)

[**1.1.2 Принципы физической защиты объектов информатизации** 9](#_Toc54900864)

[**1.1.3 Методы физической защиты объектов информатизации** 12](#_Toc54900865)

[**1.2 Анализ объектов физической защиты** 12](#_Toc54900866)

[**1.2.1 Схема анализа защищаемого объекта информатизации** 12](#_Toc54900867)

[**1.2.2 Категорирование объектов защити по уровню важности** 14](#_Toc54900868)

[**1.3 Модель угроз и модель нарушителя физической безопасности** 16](#_Toc54900869)

[**1.3.1 Возможные источники угрозы безопасности** 16](#_Toc54900870)

[**1.3.2 Модель нарушителя физической безопасности** 17](#_Toc54900871)

[**1.4 Физические средства подсистемы задержки** 18](#_Toc54900872)

[**1.4.1** **Физические барьеры** 18](#_Toc54900873)

[**1.4.2 Средства защиты окон** 19](#_Toc54900874)

[**1.5 Системы охранно-пожарной сигнализации** 20](#_Toc54900875)

[**1.5.1 Структура охранно-пожарной сигнализации** 20](#_Toc54900876)

[**1.5.2 Характеристика приемно-контрольного прибора** 21](#_Toc54900877)

[**1.5.3 Характеристика систем оповещения** 22](#_Toc54900878)

[**Список используемых источников** 24](#_Toc54900879)

# **Введение**

**Актуальность** **темы.** 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. Я НЕ ВИЖУ, ЧТО ИСПОЛЬЗОВАЛСЯ ОБРАЗЕЦ ВВЕДЕНИЯ

ГОВОРИЛИ НА ЧТО ОБРАЩАТЬ ВНИМАНИЕ

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.

**Объект исследования**, теоретические основы физической защиты объектов информатизации.

**Предмет** **исследования**, объекты информатизации.

**Цели работы и задачи исследования.** Цель работы – изучить теоретические сведения о структуре, составе и основных задачах системы физической защиты объектов, рассмотрены вопросы категорирования объектов защиты, классификации физических средств защиты подсистем обнаружения, задержки. Поставленная цель определила следующие основные задачи исследования:

1. Анализ основных теоретических положений.
2. Разработать программный проект, содержащий электронное пособие и тестовую программу по вышеуказанной теме.

**Методы исследования**. Для решения поставленных задач были использованы теоретические методы исследования. Теоретическую основу исследования составили труды Бурькова, Е. В. «Физическая защита объектов информатизации».

# **Техническое задание**

**1.1 Основание для разработки**

В связи с заданием, полученным от кафедры «Информатика» Московского технического университета связи и информатики и утвержденное научным руководителем, доцентом кафедры «Информатика» Кандидатом педагогический наук Гуриковым С.Р. 2 октября 2020 года.

**1.2 Назначение разработки**

Программный продукт предназначен для ознакомления с основными теоретическими положениями по теме курсовой работы и проверке знаний пользователя.

**1.3 Требование к программному изделию**

**1.3.1 Требование к функциональным характеристикам**

Разработанный программный продукт должен обеспечивать выполнение следующих функций:

* Возможность ознакомления с теоретическими материалами по теме курсовой работы
* Возможность проведения тестирования в соответствии полученной информации
* Возможность вывода результатов исследования для пользователя

**1.3.2 Требования к надежности**

Разрабатываемое программное обеспечение должно иметь:

* Устойчивую работу, в соответствии с алгоритмом программы
* Выдавать сообщения об ошибках
* Поддерживать диалоговый режим, в рамках предоставляемых пользователю возможностей
* Разграничения пользовательских прав
* Возможность восстановления программы после сбоя
* Защита от несанкционированного копирования

**1.3.3 Требование к составу и параметрам технических средств:**

Минимальные и рекомендуемые системные требования для ПК:

* Процессор 1 ГГц и выше;
* Оперативная память 1 Гб (для 32-bit системы) или 2 Гб (64-bit системы);
* 1 Гб свободного места на жестком диске;
* Видеокарта с поддержкой Microsoft DirectX 9 (любая современная, цена не имеет значения); ШРИФТ

1.3.4 Требование к информационной программной совместимости

Программа должна легко устанавливаться функционировать и корректно работать, при наличии следующего программного обеспечения:

* Операционная система Windows (8, 10)
* Microsoft Visual Studio CИ++

1.3.5 Требование к транспортированию и хранению

Программа поставляется на Flash-накопителе. Программная документация поставляется в электронном или печатном виде.

1.3.6 Требование к программной документации

В ходе разработки программы должны быть подготовлены: текст программы, описание программы, методика испытаний, руководство пользователя

1.3.7 Стадия и этапы разработки

**ЗДЕСЬ НАДО ЧИТАТЬ ГОСТ В ЧАСТИ ОФОРМЛЕНИЯ ТАБЛИЦ**

|  |  |  |  |
| --- | --- | --- | --- |
| №Этапа | Название этапа | Срок | Отчет |
| 1 | Утверждение темы | 02.10.2020 |  |
| 2 | Написание введения | 12.10.2020 |  |
| 3 | Написание Технического задания | 29.10.2020 |  |
| 4 | Написание теоретической части | 29.10.2020 |  |

# **Глава I. Теоретическая часть ЗДЕСЬ НАДО ЧИТАТЬ ГОСТ В ЧАСТИ ОФОРМЛЕНИЯ ТАБЛИЦ**

* 1. **Сущность и задачи физической защиты объектов информатизации**

### **1.1.1 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.

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.

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.

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

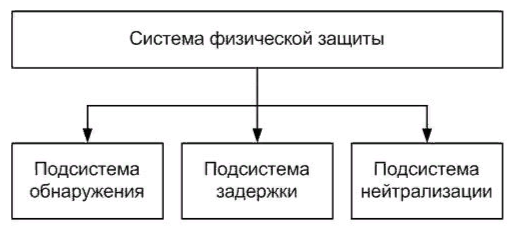


Рисунок 1.1. –Структурная схема СФЗ по решаемым задачам

Каждая из подсистем может быть реализована организационными мероприятиями, комплексом технических средств защиты и специальными подразделениями охраны. Подсистема обнаружения включает в себя охранные из вещателей, 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.

Система физической защиты в соответствии с определением, выполняемыми функциями, может быть представлена в виде совокупности инженерно-технических, организационных мероприятийи действий подразделений охраны. Структура СФЗ по составу компонентов представлена на рисунке 1.2.

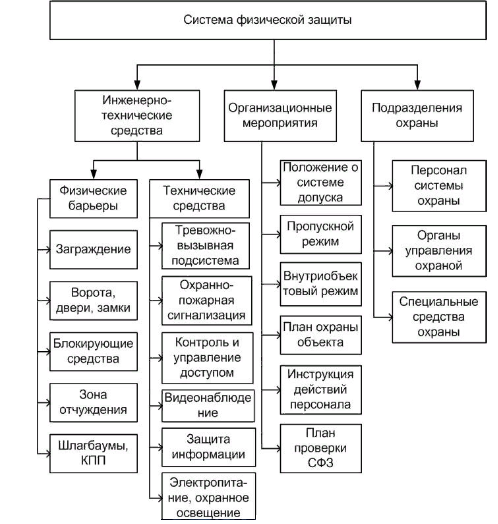


Рисунок 1.2 –Структура СФЗ по составу компонентов

**РИСУНКИ ЧЕРТЯТСЯ СТУДЕНТОМ**

**ЗНАЧИТ ТАК, ПЕРЕЧИТЫВАЕТЕ КОНСПЕКТ И ПРОЧИЙ МАТЕРИАЛ, ГОСТЫ**

**И ПОТОМ БУДЕМ ПРОВЕРЯТЬ**

**1.1.2 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;

−равно прочность рубежа контролируемой зоны;

−ограниченный доступ к элементам системы защиты;

−адаптируемость системы защиты к новым угрозам;

−согласованность системы защиты с другими системами организации;

**Непрерывность физической** защиты определяет постоянную готовность системы защиты к нейтрализации угроз.

**Надежность защиты** подразумевает обеспечение требуемого уровня безопасности объекта независимо от внешних и внутренних факторов.

**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.

**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.

**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.

**Вложенные зоны** наиболее распространены, так как позволяют экономно обеспечить требуемый уровень безопасности.

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

**Равнопрочность рубежа контролируемой зоны**–это принцип эффективной защиты, заключающийся в том, что 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.

**1.1.3 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.

Методы физической защиты объектов:

−создание физических, электронных и других препятствий злоумышленнику на пути к носителям конфиденциальной информации и ее источниками 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.

**1.2 Анализ объектов физической защиты**

**1.2.1 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.

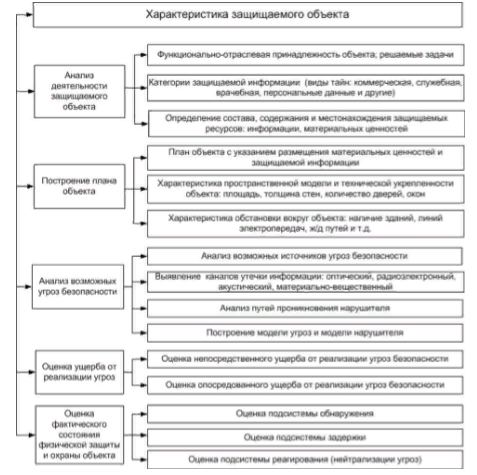


Рисунок 2.1 –Схема анализа защищаемого объекта

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 пожаров-и взрывоопасности, по виду потерь, по масштабу потенциальных потерь, по объему производства, по количеству персонала и т.д.

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, связанные 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).

**1.2.2 Категорирование объектов защити по уровню важности**

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

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, 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 аптек управления, аптеки, склады мед резерва, 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.
* специальные помещения объектов особо важных и повышенной опасности.

**−объекты группы Б:** важные объекты, хищения на которых могут привести к ущербу в размере свыше 500 МРОТ.

* 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).
* 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.

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.

## **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;

–сбоив работе средств СФЗ;

–воздействие субъективного фактора.

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.

### **1.3.1 Возможные источники угрозы 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 политическими событиями.

**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.



Рисунок 3.1 –Источники угроз физической безопасности

### **1.3.2 Модель нарушителя физической безопасности**

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

**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).

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.

## **Физические средства подсистемы задержки**

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

### **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.

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.

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.4

**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.

### **1.4.2 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.

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.

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.

## **1.5 Системы охранно-пожарной сигнализации**

**Охранно-пожарная сигнализация**—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.

### **1.5.1 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 магнит контактных 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.

### **1.5.2 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 из вещателей, 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 повышателями и индикаторами. Кроме того, приборы обеспечивают сдачу и снятие объекта с охраны по принятой тактике, а в ряде случаев —электропитание извещателей.

**Шлейф сигнализации** является одной из необходимых составных частей объектовой системы охранно-пожарной сигнализации. 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 извещателей электропитания

**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 из вещателя, работоспособность которого можно проверить только во время технического обслуживания ОПС.

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

**Адресные не опросные системы** являются, по сути, пороговыми, дополненными лишь возможностью передачи кода адреса, сработавшего извещателя.

**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.

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.

### **1.5.3 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.

**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

—своевременно передавать информацию о возникновении пожара,

—способствовать реализации плана эвакуации людей с объекта.

**Таким образом**, по итогам работы над 1 главой, можно сказать, что были успешно проанализированы основные теоретические положения. Обозначены детали работы физической защиты объектов информатизации, а также подтверждена актуальность данной темы. На основе всего этого в дальнейшем будет разработана тестовая программа на языке С++ в среде Visual Studio, по материалам, описанным выше.

# **Список используемых источников**

1 ГОСТ 7.1-2003. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления [Текст]. – Введ. 2004-07-01. - Минск.: Межгос. совет по стандартизации, метрологии и сертификации; М.: Госстандарт России: Изд-во стандартов, 2004. – 166 с.

2 Бурькова, Е. В. Физическая защита объектов информатизации: учебное пособие / Е. В. Бурькова. — Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017. — 158 c. — ISBN 978-5-7410-1697-8. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/71349.html (дата обращения: 29.10.2020). — Режим доступа: для авторизир. пользователей