Воронежский институт МВД России

Кафедра радиотехнических систем и комплексов охранного мониторинга

Допущен к защите
Начальник кафедры
радиотехнических систем и
комплексов охранного мониторинга
кандидат технических наук
полковник полиции

С.А. Гречаный
«____»_____ 2020 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: «Разработка комплексной системы охраны офисного здания»

Исполнитель:	слушатель 314О учебной группы специальность 11.05.02 – «Специальные радиотехнические системы» прапорщик полиции Мироненко Н.П.	_____ (подпись)
Руководитель:	преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга кандидат технических наук майор полиции Меркулова Н.И.	_____ (подпись)
Рецензент:	доцент кафедры информационной безопасности кандидат технических наук полковник полиции Алексеенко С.П.	_____ (подпись)

Воронеж
2020

СОДЕРЖАНИЕ

Задание на выпускную квалификационную работу…… 4
Реферат……..... 7
Введение…….. 8
Глава 1. Анализ использования комплексных систем безопасности…… 10
1.1. Понятия и основные признаки КСБ…… 10
1.2. Способы обнаружения нарушителей при проникновении на объект……..... 15
Глава 2. Выбор интегрированной системы безопасности…….. 18
2.1. Выбор интегрированной системы безопасности методом экспертных оценок……..... 18
2.2. Выбор интегрированной системы безопасности методом парного сравнения…….. 23
Глава 3. Основные технические решения по построению комплексной системы безопасности офисного здания…….. 26
3.1. Система охранно-тревожной сигнализации и контроля и управления доступом……. 26
3.2. Система охранная телевизионная……... 31
3.3. Выполнение требований по технике безопасности и охране труда при выполнении работ по внедрению комплексной системы безопасности……..... 39
Глава 4. Комплексные системы безопасности…… 40
4.1. Определение, задачи и функциональные возможности комплексных систем безопасности…….. 40
4.2. Система безопасности на базе прибора приемно-контрольного охранно-пожарного «Кодос А-20»……... 44
4.3. Интегрированный комплекс технических средств охраны «Пахра»…… 45
4.4. Интегрированная система безопасности «Рубеж-08»……. 47

4.5. Интегрированная система безопасности «Стрелец-Интеграл»…… 48
Глава 5. Расчет технических параметров комплексной системы безопасности офисного здания……..…….. 51
5.1. Расчет электропитания систем охранно-тревожной сигнализации и контроля управления доступом…… 51
5.2. Расчет электропитания систем охранно-тревожной сигнализации и контроля и управления доступом…….. 54
5.3. Расчет параметров сигнальной линии связи в комплексной системе безопасности……..……..... 56
Заключение……. 60
Список литературы…….……... 61

УТВЕРЖДАЮ
Начальник кафедры
радиотехнических систем и
комплексов охранного мониторинга
кандидат технических наук
полковник полиции
С.А. Гречаный
«____»_____ 20__ г.

ЗАДАНИЕ

на выпускную квалификационную работу слушателю

прапорщику полиции Мироненко Никите Павловичу

(специальное звание, фамилия, имя, отчество)

Руководитель: преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга кандидат технических наук майор полиции Меркулова Наталья Ивановна

(должность, учёное звание, специальное звание, фамилия, имя, отчество)

1. Тема выпускной квалификационной работы: «Разработка комплексной системы охраны офисного здания». Утверждена приказом начальника Воронежского института МВД России от «___»_____20__г. № ___.

2. Цель выпускной квалификационной работы: разработать комплекс мероприятий по построению комплексной системы безопасности офисного здания.

3. Срок сдачи выпускной квалификационной работы: «___»_____20__г.

4. Исходные данные к выпускной квалификационной работе:

- план-схема объекта;
- перечень используемого оборудования;
- условные графические обозначения технических средств охраны и безопасности;
- нормативные правовые и нормативно-технические документы;
- справочная литература.

5. Перечень подлежащих разработке вопросов:

- провести анализ нормативной базы по обеспечению безопасности офисного здания;
- провести анализ угроз безопасности офисного здания. Подготовить техническое задание на проектирование системы охранной телевизионной, системы охраны периметра и системы контроля и управления доступом офисного здания;

- разработать структурную схему системы охранной телевизионной, системы охраны периметра и системы контроля и управления доступом офисного здания;

- провести расчет электропитания системы охранной телевизионной, системы охраны периметра и системы контроля и управления доступом офисного здания.

6. Перечень обязательного графического материала:

- структурные схемы (системы охранной телевизионной, системы контроля и управления доступом);

- планы расположения оборудования;

- результаты расчетов (параметров системы охранной телевизионной, системы контроля и управления доступом офисного здания).

7. Литература к заданию:

- Конституция Российской Федерации от 12 декабря 1993 г. (принята всенародным голосованием 12 декабря 1993 г.) [Электронный ресурс]. – Режим доступа: http://www.garant.ru/doc/constitution/.

- Вопросы Федеральной службы войск национальной гвардии Российской Федерации: указ Президента Российской Федерации от 5 апреля 2016 г. № 157 [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/420346527.

- О войсках национальной гвардии: федеральный закон от 3 июля 2016 года № 226-ФЗ.

- О противодействии терроризму: федеральный закон от 6 марта 2006 г. № 35-ФЗ [Электронный ресурс]. – СПС «Консультант плюс». – URL : http // www.base.consultant. ru.

- ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. – Введ. 2016-01-01. – Москва : Стандартинформ, 2014. – 27 с.

- СП 132.13330.2011. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования.

- СП 5.13130.2009. Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования.
- Правила устройства электроустановок (Утверждены Приказом Минэнерго России от 08 июля 2002 г. № 204). – М.: Энергоатомиздат, Изд. 7., 2002. – 222 с.
- ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования. Введ. 2010-09-01. – Москва : Стандартинформ, 2010. – 32 с.
- Сидоров А.В. Процедура выбора оптимальной системы охраны при обеспечении охраны объекта // Охрана, безопасность, связь. – 2017 – №1-1. – С. 164-167
- Винокуров С.А. Организация интегрированных систем безопасности и охранного мониторинга : курс лекций. Ч.1 / С.А. Винокуров, С.А. Гречаный, М.Ю. Пакляченко. – Воронеж: Воронежский институт МВД России, 2019. – 165 с.
- Винокуров С.А. Организация интегрированных систем безопасности и охранного мониторинга : курс лекций. Ч.2 / С.А. Винокуров, С.А. Гречаный, М.Ю. Пакляченко. – Воронеж: Воронежский институт МВД России, 2019. – 158 с.
- Ворона В.А. Комплексные интегрированные системы обеспечения безопасности [Электронный ресурс]: учебное пособие / Ворона В. А., Тихонов В. А. – Электрон. Текстовые данные. – Москва: Горячая линия-Телеком, 2013. – 160 с. – Режим доступа: http://www.iprbookshop.ru/11989/ - ЭБС «IPRbooks», по паролю.

Задание выдал:
преподаватель кафедры
радиотехнических систем и
комплексов охранного мониторинга

кандидат технических наук _____ Н.И. Меркулова
майор полиции
«___»_____20___г.
(подпись)

Задание получил:
слушатель 314О учебной группы
факультета заочного обучения
прапорщик полиции
«___»_____20___г. _____ Н.П. Мироненко
(подпись)

С Положением о государственной итоговой аттестации выпускников Воронежского института МВД России, утвержденным приказом начальника института от «15» мая 2017 г. № 475, ознакомлен.

_____
(подпись курсанта (слушателя), фамилия, имя, отчество)

РЕФЕРАТ

Пояснительная записка: 63 страницы, 6 рисунков, 27 источника литературы, 6 приложений.

Ключевые слова: комплексная безопасность, интегрированная система безопасности, охранно-пожарная сигнализация, система контроля и управления доступом, система охранная телевизионная, интеграция,

Объект исследования: комплексная система безопасности офисного здания.

Цель работы: разработать проектно-сметную документацию на комплексную систему безопасности офисного здания.

Для достижения поставленной цели использовался комплекс общих и частных методов, среди которых анализ; описание; автоматизированное проектирование.

Полученные результаты: разработан комплект проектно-сметной документации на комплексную систему безопасности офисного здания с использованием оборудования «Кодос», объединяющую системы охранной и пожарной сигнализации, контроля и управления доступом, охранную телевизионную.

Главной задачей в выпускной квалификационной работе является:

- проанализировать сведения о состоянии современных систем безопасности;
- проанализировать нормативную базу по обеспечению охраны офисного здания;
- проанализировать угрозы охраны офисного здания
- разработать техническое задание на проектирование комплексной системы охраны;
- рассчитать и оценить надежность комплексной системы охраны объекта.

ВВЕДЕНИЕ

В соответствии с Федеральным законом от 31 мая 2002 г. № 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" адвокатская деятельностью является квалифицированная юридическая помощь, оказываемая на профессиональной основе лицами, получившими статус адвоката физическим и юридическим лицам в целях защиты их прав, свобод и интересов, а также обеспечения доступа к правосудию. Очевидно, что для подразделений вневедомственной охраны важно

обеспечить охрану данных объектов на высоком уровне, так как преступные посягательства на подобные объекты могут привести к негативным материальным последствиям, как для собственника (коммерческая организация), так и для государства (государственная организация), и привести к утечке конфиденциальной информации, составляющие персональные данные граждан. Особую актуальность обеспечение безопасности объектов приобрело в последнее время, когда на Российскую Федерацию стало оказываться колоссальное давление со стороны иностранных государств в различных сферах деятельности (политической, экономической, военной, информационной). При этом существующая социально-экономическая обстановка в стране непростая с учетом введения некоторыми странами санкций в отношении РФ, ослабления национальной валюты, кризисных явлений на внешнем и внутреннем рынках, недостатка бюджетного финансирования и проблем обеспечения социальных и финансовых трудностей субъектов предпринимательской деятельности, сокращения доходов и покупательской способности граждан.

В офисе адвокатуры будут установлены системы охранной-тревожной, пожарной, охранная телевизионная для обеспечения защиты объекта от противоправных посягательств.

Для безопасности персонала и посетителей охраняемый объект будет оборудован системой охранно-тревожной сигнализации. Предупреждение пожаров выполняет система пожарной сигнализации, представленная дымовыми оптико-электронными и ручными пожарными извещателями.

Для наблюдения и записи происшествий объект оборудован системой охранной телевизионной, представленной телевизионными камерами. В ночное время автоматически включаются инфракрасные подсветки видеокамер.

Оборудования офиса адвокатуры системами охранно-тревожной, пожарной, охранной телевизионной предусматривает разработку

проектно-сметной документации. Монтаж системы безопасности производят по утвержденным проектам и сметам, которые разрабатывают проектные организации. Состав проектно-сметной документации:

- техническое задание;
- пояснительная записка;
- поэтажные планы размещения элементов системы охраны;
- структурные схемы организации системы охраны;
- спецификация оборудования (изделий и материалов) систем;
- документы рабочего проекта.
- расчеты необходимых характеристик по обеспечению
- работоспособности и эксплуатации оборудования;
- таблица исходных данных для программирования технических средств охраны;
- чертежи общих видов нетиповых решений, конструкций и оборудования

В данной выпускной квалификационной работе будет разработана проектно-сметная документация на системы охранно-тревожной, пожарной сигнализаций и систему контроля и управления доступом офисного здания

ГЛАВА 1. АНАЛИЗ ИСПОЛЬЗОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

1.1 Понятие и основные признаки КСБ

«Акт незаконного вмешательства – противоправное действие (бездействие), в том числе террористический акт или покушение на его совершение, угрожающее безопасному функционированию объекта, повлекшее за собой причинение вреда жизни и здоровью людей, повреждение или уничтожение имущества либо создавшее угрозу наступления таких последствий».

Суть концепции обеспечения комплексной безопасности офисного здания поясняется на рис. 1.1 и заключается в реализации трех принципов:

– определение целей (предметов) защиты (кого и что защищать);

– определение и оценка угроз (от кого защищать);

– разработка и реализация адекватных мер защиты (как защищать).

– рассмотрим подробнее элементы этой концепции. На охраняемом объекте в самом общем случае можно выделить три цели защиты:

– люди (персонал объекта, население прилегающей территории);

– имущество (оборудование, ценности, документация);

– информация (государственная тайна, конфиденциальная, служебная или коммерческая информация). Цели защиты образуют пространство угроз.

Под угрозой безопасности охраняемому объекту следует понимать совокупность определенных, непредумышленных или заранее запланированных, намерений, условий и факторов, реализация и осуществление которых могут привести к нарушению целостности данного объекта и, следовательно, к неэффективности предпринимаемых с целью его защиты организационно-служебных, инженерно-технических, информационных и других мер и мероприятий.

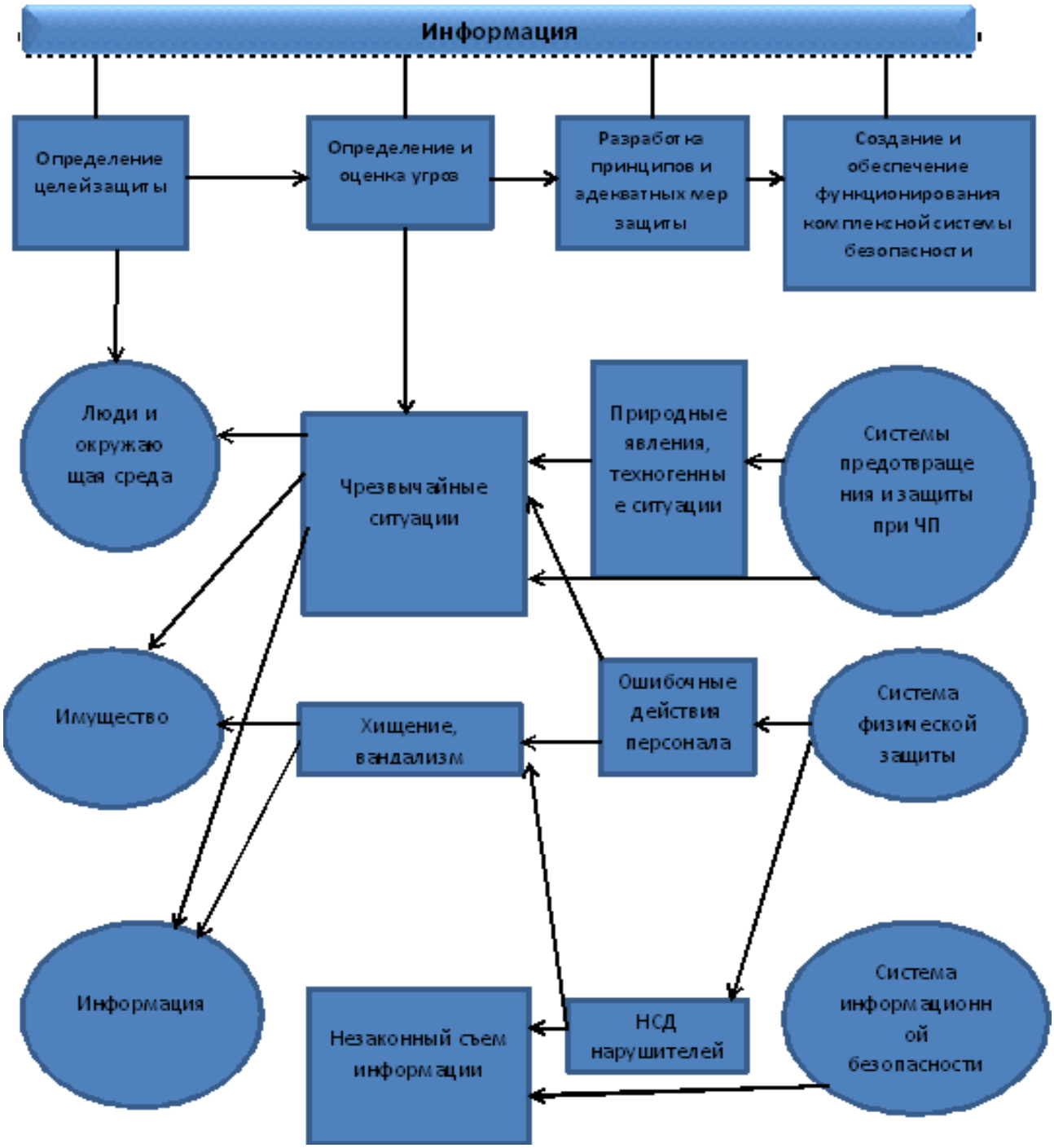

Рис. 1.1. Концепция обеспечения комплексной безопасности объекта

Меры защиты от угроз должны предусматривать:

– тотальный контроль несанкционированного проникновения на территорию объекта, в здания и помещения;

– ограничение и контроль доступа людей в режимные здания и помещения с возможностью документирования результатов контроля;

– обнаружение нарушителей на самых ранних этапах;

– оценку ситуации;

– создание на пути продвижения нарушителя физических препятствий, обеспечивающих задержку, необходимую силам охраны для его задержания;

– принятие немедленных действий по развертыванию сил охраны и пресечению нарушения;

– видеодокументирование действий персонала на особо ответственных участках объекта.

Система обеспечения комплексной безопасности объекта должна быть сформирована таким образом, чтобы с помощью людей и технических средств эффективно противостоять перечисленным угрозам путем принятия адекватных мер защиты.

Для этого должны создаваться и надежно функционировать следующие подсистемы безопасности:

– система защиты объекта при чрезвычайных ситуациях;

– система физической защиты (охраны);

– система информационной безопасности.

Для определения требуемого уровня защищенности объекта (способности его противостоять действиям нарушителя) необходимо формирование модели нарушителя, на способности и возможности которого должна ориентироваться создаваемая КСБ.

Модель нарушителей – совокупность сведений о численности, оснащенности, подготовленности, осведомленности и тактике действий нарушителей, их мотивации и преследуемых ими целях, которые используются при выработке требований к системе физической защиты и оценке ее эффективности. В самом общем виде модель нарушителя может выглядеть как на рис. 1.2.

Способы проникновения нарушителя на объект обладают информационными признаками, которые должны использоваться для

определения каналов проникновения.

На основании статистики нарушений режима, установленного на объекте, и анализа окружающей его криминогенной обстановки, а также оценки возможностей круга заинтересованных в НСД к охраняемому имуществу лиц (организаций), составляется образ (модель) наиболее вероятного нарушителя. Такая модель наделяется максимальными для выбранного типа способностями и возможностями по преодолению КСБ. Созданная модель нарушителя принимается как базовая и относительно нее проходит разработка КСБ. Определение целей вторжения на территорию объекта, модели наиболее вероятного нарушителя и наиболее вероятных сценариев его действий дает возможность сформировать требования к КСБ (например, к системе защиты периметра (СЗП)), при реализации которых возможно ее эффективное противостояние существующим угрозам.

Созданная модель нарушителя принимается как базовая и относительно нее проходит разработка КСБ. Таким образом:

1. Модель угроз определяет всю совокупность путей и способов реализации угроз охраняемому объекту.

2. Нарушитель является средством реализации внешних искусственных угроз охраняемому объекту.

3. Модель нарушителя определяет всю совокупность характеристик нарушителя, а также способов его проникновения на охраняемый объект.

4. Модель нарушителя дает возможность определить каналы проникновения и сформировать требования к инженерно-техническим средствам системы охраны.

Характеристики охраняемого объекта в основном отражают цели проникновения нарушителя и определяют степень защищенности объекта от угроз. Расположение охраняемого объекта влияет на степень защищенности объекта от угроз и способы проникновения нарушителя на объект. Модель угроз определяет всю совокупность путей и способов

реализации угроз охраняемому объекту и отражает наиболее вероятные угрозы.

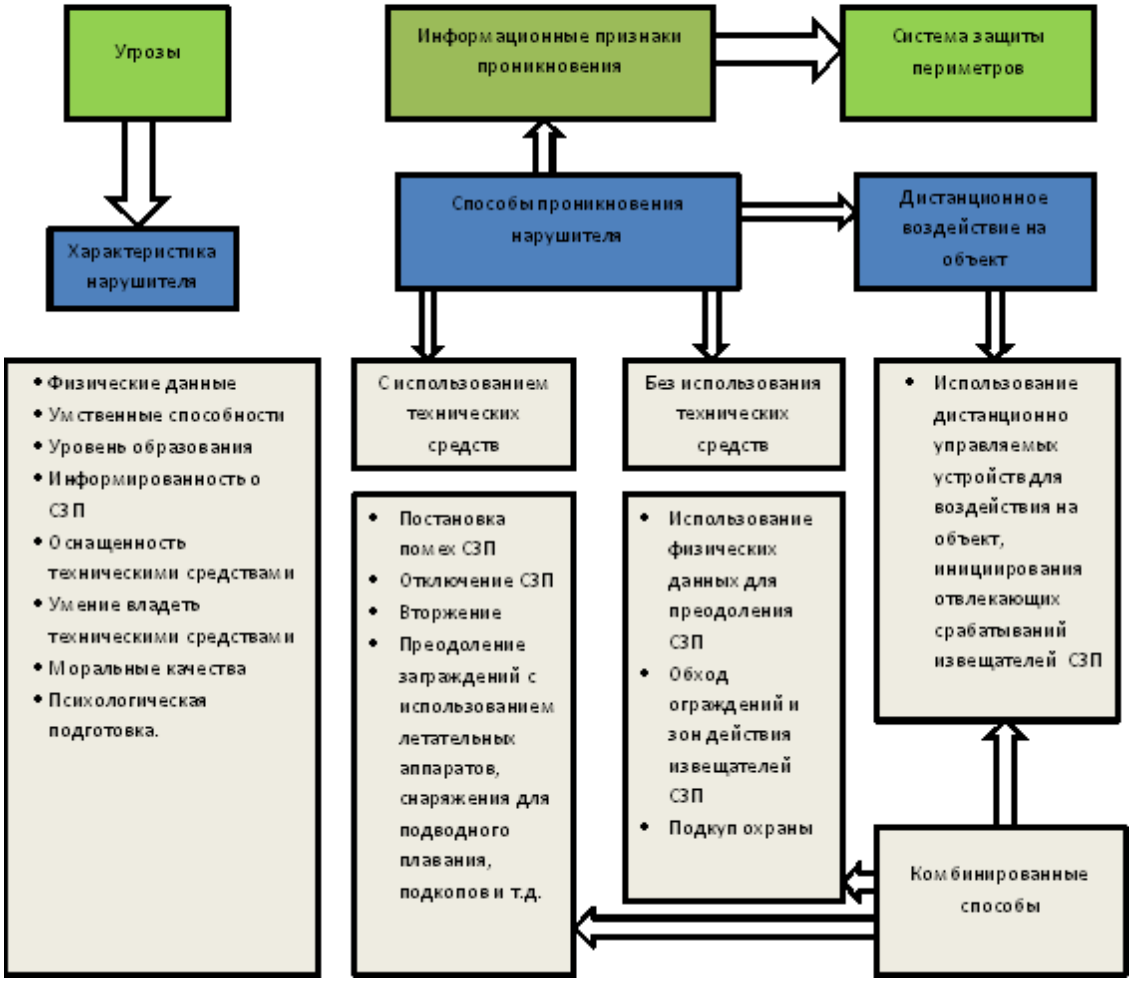

Рис. 1.2. Общий вид модели нарушителя

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

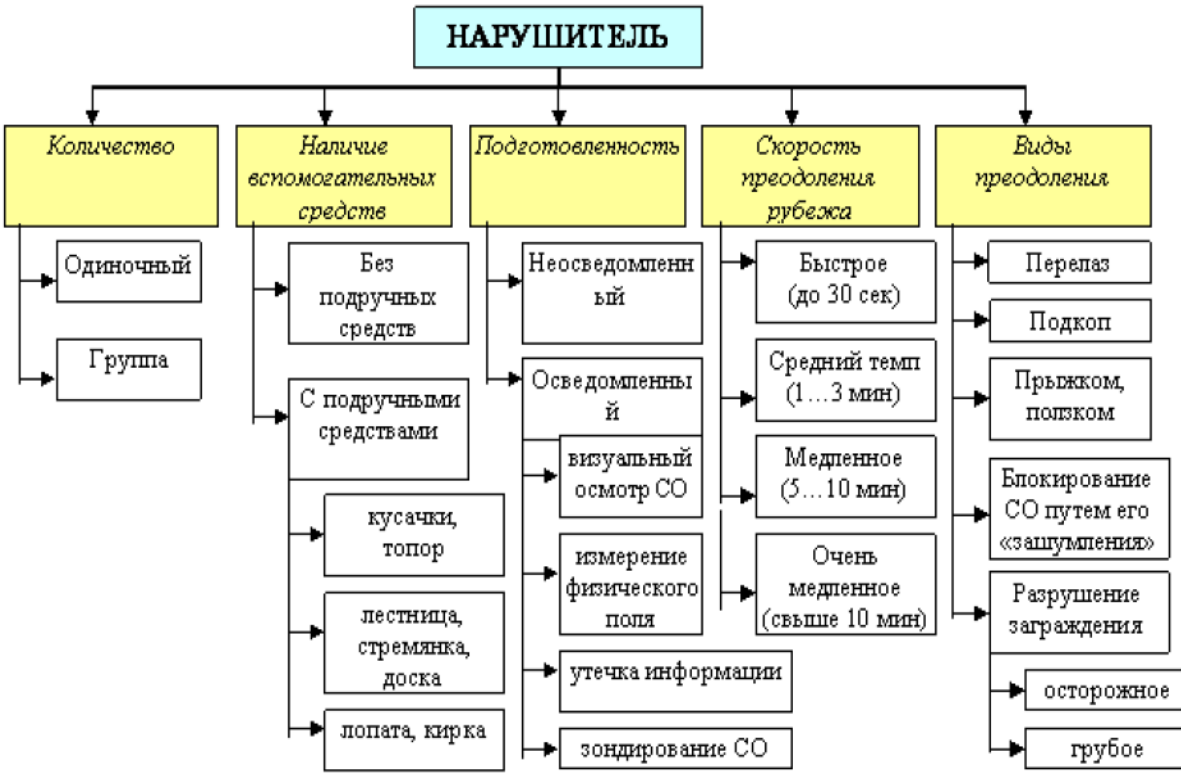

Рис. 1.3. Классификация нарушителей

1.2. Способы обнаружения нарушителя при проникновении на охраняемый объект

Способы обнаружения нарушителя определяются в основном, исходя из всей совокупности информационных признаков проникновения нарушителя. Признаки проникновения нарушителя, отражающие возмущения, производимые им во внешней среде при преодолении СЗП, зависят от свойств нарушителя, как материального объекта. Свойства нарушителя определяются из модели нарушителя и полностью могут быть описаны его характеристиками. В свою очередь, свойства нарушителя значительно зависят от использования нарушителем технических средств, применяемых им при проникновении на охраняемый объект. Технические средства, как правило, расширяют возможности нарушителя по преодолению СЗП, придают ему новые свойства, но и в то же время их

функционирование может служить дополнительными признаками проникновения. Кроме того, использование технических средств повышает стоимость реализации угроз. В самом общем случае, структура формирования способов обнаружения нарушителя будет иметь вид как показано на рисунке 1.4.

В конечном счете, поскольку задачей системы охраны является оказание противодействий нарушителю в достижении его целей, при построении системы охраны в ее структуру закладывается принцип создания последовательных рубежей на пути движения нарушителя. Угроза проникновения обнаруживается на каждом рубеже и ее распространению создается соответствующая преграда. Такие рубежи располагаются последовательно от прилегающей к зданию территории до охраняемого помещения, сейфа. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по минимальному значению времени, которое нарушитель затратит на преодоление всех зон безопасности. За это время, с вероятностью близкой к 1, должна сработать система охранной сигнализации. Сотрудники охраны установят причину тревоги и примут необходимые меры.

В зависимости от того, использует нарушитель технические средства при проникновении или нет, информационные признаки проникновения могут быть различными. Знание наиболее вероятных каналов проникновения позволит выбрать соответствующие способы обнаружения нарушителя при формировании конкретной структуры КСБ.

Основные свойства нарушителя, не использующего технические средства, информационные признаки проникновения нарушителя и способы его обнаружения представлены в табл. А.1 приложения А.

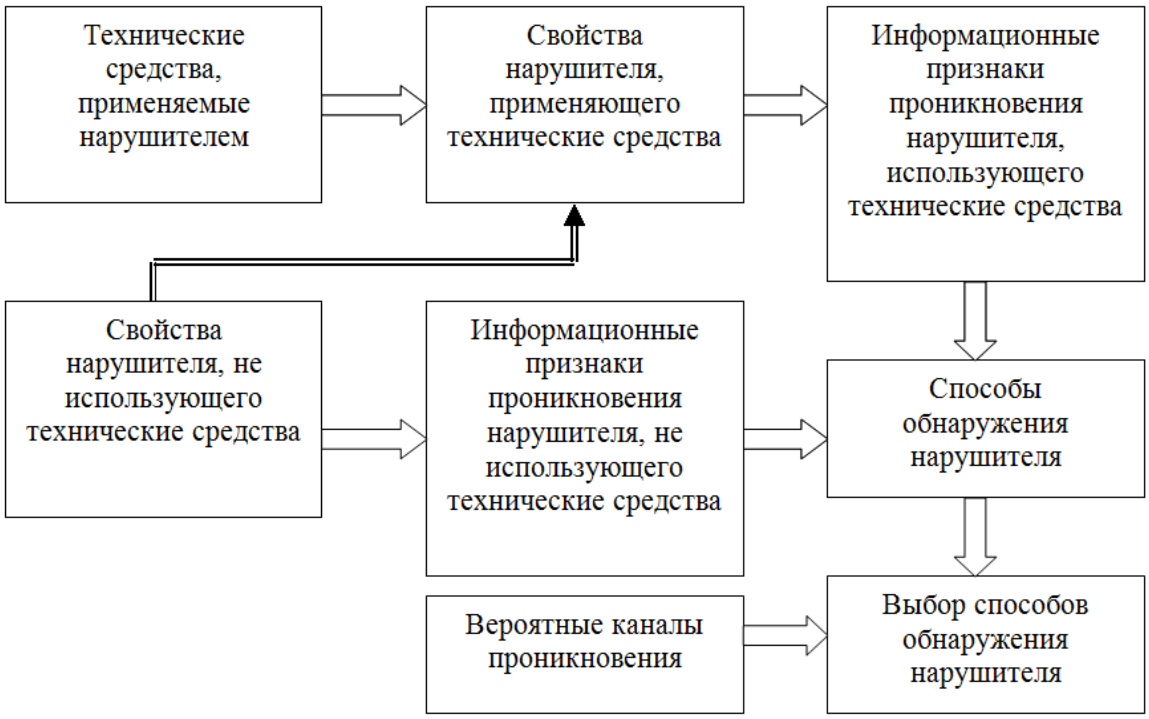

Рис. 1.4. Структура формирования способов обнаружения нарушителя

Таким образом, основные способы обнаружения нарушителя:

– обнаружение нарушителя по фиксированию удельного давления на грунт;

– обнаружение нарушителя по фиксированию сейсмических колебаний грунта;

– обнаружение нарушителя по фиксированию нарушений целостности грунта, обнаружение нарушителя по фиксированию акустических колебаний заграждения при его преодолении;

– обнаружение нарушителя по фиксированию изменений электрических и магнитных характеристик пространства;

– обнаружение нарушителя по фиксированию ИК – излучения человека;

– обнаружение нарушителя по зафиксированным с помощью СТН формам, размерам и параметрам движения объекта наблюдения;

– обнаружение нарушителя по фиксированию СВЧ сигнала,

отраженного от нарушителя и искаженного им;

– обнаружение нарушителя по фиксированию факта прерывания луча ИК излучателя;

– обнаружение нарушителя по фиксированию ультразвуковых импульсов, отраженных от нарушителя;

– фиксирование признаков работы технических средств (акустическое и электромагнитное излучение).

Для эффективного обнаружения возможных угроз система охраны периметра в составе КСБ объекта ТЭК должна базироваться на ряде принципов:

– принцип непрерывности рубежа обнаружения. Периметр делится на участки для облегчения обнаружения и последующего целеуказания при реагировании. Датчики должны формировать по периметру непрерывную линию обнаружения. На практике это означает такое расположение технических средств, чтобы зона обнаружения одного датчика пересекалась с зонами обнаружения двух смежных сенсоров;

– принцип эшелонированной защиты. Концепция эшелонированной защиты подразумевает использование нескольких рубежей обнаружения. Использование нескольких рубежей обнаружения позволяет повысить надежность и отказоустойчивость, а также улучшить вероятностные характеристики системы.

– принцип ортогональности датчиков обнаружения. Для повышения достоверности принятия решения о вторжении на охраняемый объект применяются различные типы датчиков обнаружения.

Таким образом, в первой главе выпускной квалификационной работы был приведены результаты изучения и анализа концепции обеспечения комплексной безопасности офисных зданий, особое внимание при этом уделено организации защиты их периметров.

ГЛАВА 2. ВЫБОР ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

2.1. Выбор интегрированной системы безопасности методом экспертных оценок

При выборе ИСБ следует обратить на целый ряд требований, в соответствии с ГОСТ Р 56875-2016:

– ИСБ должны быть восстанавливаемыми изделиями и рассчитаны на непрерывную круглосуточную работу по ГОСТ 27.002-2015;

– ИСБ следует проектировать на основе функциональных задач, позволяющих формировать направляемые блоки, образующие ИСБ с заданной конфигурацией, обеспечивающие возможность ее развития функциональных возможностей под конкретные условия практического применения на объекте по ГОСТ Р 57674-2017.

Из большого обилия ИСБ необходимо выбрать наиболее подходящую систему. Для этого существует большое разнообразие способов выбора систем.

Сейчас довольно популярны методы экспертных оценок. Выбирать ИСБ можно либо на основе объективных данных, либо на основе мнений специалистов (экспертов). Существует две группы экспертных оценок:

- индивидуальные оценки, предполагают выставление оценки на основе мнения отдельных экспертов, независимых друг от друга;
- коллективные оценки, основаны на анализе коллективного мнения опрошенных экспертов.

Рассмотрим несколько способов сравнения объектов, в частности характеристик ИСБ. Ранжирование — это упорядоченное размещение объектов в порядке возрастания или убывания по какому-то присущему им

признаку. Ранжирование позволяет выбрать из сравниваемой группы объектов наилучший вариант.

Парное сравнение — это нахождение наиболее важного значения объектов при сравнении всех возможных пар. Следует из каждой пары выявить более значимый объект или установить их равенство.

Метод непосредственной оценки бывает желательным не только в упорядочивании, но и в определении, на сколько один фактор более предпочтителен, чем другие. В этом случае широта изменения характеристик объекта разбивается на отдельные промежутки, каждому из которых присваивается определенная оценка (балл), например, от 0 до 10.

Метод простой ранжировки заключается в том, что каждого эксперта просят расположить признаки в порядке предпочтения по возрастанию или убыванию. Для некоторых методов удобно использовать таблицу, куда будут вносится данные.

Пример матрицы сравниваемых объектов представлен в таблице 2.1.

Таблица 2.1.

Матрица сравниваемых объектов

№ п/п	1	2	…	J	…	m
1	a_{11}	a_{12}	…	a_{1j}	…	a_{1m}
2	a_{21}	a_{22}	…	a_{2j}	…	a_{2m}
…	…	…	…	…	…	…
I	a_{i1}	a_{i2}	…	a_{ij}	…	a_{im}
…	…	…	…	…	…	…
N	1_{ni}	a_{n2}	…	a_{nj}	…	a_{nm}

a_{ij} – оценка признака экспертом. n – количество признаков, m – количество экспертов.

Затем, подсчитывается S_i, – среднее значение важности признака. Далее представлена последовательность алгоритма метода определения весовых коэффициентов.

Метод определения весовых коэффициентов (a_{ij}):

– всем сравниваемым характеристикам назначают весовые коэффициенты;

– наиболее важной из всех сравниваемых характеристик назначают весовой коэффициент, равный какому-то фиксированному числу (наивысшему), а всем остальным – коэффициенты, равные сотым долям этого числа.

Метод последовательных сравнений заключается в следующем:

– эксперт расставляет все исследуемые характеристики в порядке уменьшения их значимости: $A1>A2>\ldots>A_n$;

– присваивает первой характеристике значение, равное единице: $A_1=1$, остальным же характеристикам назначает весовые коэффициенты в долях единицы;

– сравнивает значение первой характеристики с суммой всех последующих;

– наиболее важной из всех сравниваемых характеристик назначают весовой коэффициент, равный какому-то фиксированному числу (наивысшему), а всем остальным – коэффициенты, равные сотым долям этого числа.

При использовании метода парного сравнения чаще всего составляется матрица размером n на n, где n – количество сравниваемых характеристик.

Пример матрицы заполнения объектов при парном сравнении представлен в таблице 2.2.

Таблица 3.2.

Матрица заполнения объектов при парном сравнении

№ п/п	1	2	…	J	…	n
1	a_{11}	a_{12}	…	a_{1j}	…	a_{1n}
2	a_{21}	a_{22}	…	a_{2j}	…	a_{2n}
…	…	…	…	…	…	…
I	a_{i1}	a_{i2}	…	a_{ij}	…	a_{in}
…	…	…	…	…	…	…
N	1_{ni}	a_{n2}	…	a_{nj}	…	a_{nn}

При сравнении объектов матрица заполняется характеристиками a_{ij} следующим образом (может быть предложена и иная схема заполнения):

– 2, если характеристика i предпочтительнее характеристики j (i > j);

– 1, если установлено равенство характеристик (i = j);

– 0, если характеристика j предпочтительнее характеристики i (i < j).

Для обработки и анализа результатов применяются различные методы математической статистики. Причем, они могут комбинироваться и меняться в зависимости от типа задачи и необходимого результата.

Итак, пусть группа экспертов оценила какую-либо характеристику, тогда x_j – оценка j-го эксперта, где m – число экспертов.

Для формирования обобщенной оценки группы экспертов чаще всего используются средние величины. Например, медиана, за которую принимается такая оценка, по отношению к которой число больших оценок равняется числу меньших.

Иногда требуется определить, насколько та или иная характеристика важна с точки зрения какого-либо критерия (параметра). В этом случае

говорят, что нужно определить вес каждого фактора. Он отличается от формирования обобщенной оценки тем, что определяется не общая оценка характеристики, а оценка для каждого ее признака.

Существует большое множество возможных методов обработки оценок. Например, один из возможных вариантов, это использовать систему рейтинга Эло для метода парных сравнений. Коэффициент Эло – это метод расчёта относительной силы определенных параметров, в которых участвуют два сравниваемых объекта.

В случае участия в опросе нескольких экспертов, очевидно их расхождение во мнении, однако величина этого расхождения имеет важное значение, и в дальнейшем происходит расчет среднего значения. Групповая оценка может считаться достаточно надежной только при условии хорошей согласованности ответов.

Для анализа разброса и согласованности оценок применяются статистические характеристики – меры разброса или статистическая вариация.

Способы вычисления меры разброса:

– вариационный размах:

$$R = x_{max} - x_{min}; \tag{2.1}$$

– среднее линейное отклонение:

$$a = \frac{1}{n}\sum_{i=1}^{n}|x_i - \bar{x}|; \tag{2.2}$$

– среднеквадратическое отклонение:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}; \tag{2.3}$$

– дисперсия:

$$\sigma^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - x)^2; \qquad (2.4)$$

Коэффициент (величина ρ) может изменяться в диапазоне от –1 до +1. При полном совпадении оценок коэффициент равен единице. Равенство коэффициента -1 наблюдается при наибольшем расхождении во мнениях отдельных специалистов. экспертов. x_{ij} – ранг (важность), присвоенный i-му объекту j-ым экспертом, x_{ik} – ранг, присвоенный i-му объекту k-ым экспертом, d_i – разница между рангами, присвоенными i-му объекту.

Коэффициент конкордации Кенделла может принимать значения в пределах от 0 до 1. При полном совпадении мнений экспертов коэффициент конкордации равен единице при полном разногласии – нулю. Наиболее реальным является случай частичной согласованности мнений экспертов.

2.2. Выбор интегрированной системы безопасности методом парного сравнения

Метод парного сравнения – один из инструментов оценки и выбора решений, широко используется в экспертных оценках при необходимости расставлять приоритеты в процессе какой-либо деятельности или ранжирования различных объектов.

Идея метода состоит в том, что попарно сравниваются каждые два объекта и определяется первенство одного из них, отсюда название – «попарное (или парное) сравнение». Считается, что при решении проблемы гораздо легче сделать качественное сравнение двух объектов, опираясь на мнение экспертов, чем установить количественные критерии.

Для использования метода парного сравнения необходимо сначала определить характеристики интегрированных систем безопасности по

которым будет идти сравнение и узнать их значения. Лучше всего это представить в таблице.

Если первый параметр превосходит второй параметр, то первому параметру присваивается 1 балл, второму – 0. Если значения равны – 0,5 баллов. После чего рассчитывается сумма всех оценок и средние значения оценок попарного сравнения двадцати параметров интегрированных систем безопасности по формуле (2.5). Счет идет по строкам, слева направо. По формуле (2.6) вычисляется сумма баллов оценки присвоенных всем параметрам. Высчитывается значение нормированного весового коэффициента j=1 параметра по формуле (2.4). Округление происходит до двух знаков после запятой.

По итогам получения значения обобщенного весового коэффициента параметров найдем коэффициент оптимальности $К_{опт}$ для каждой ИСБ. По формуле 3.9 определим наиболее оптимальную ИСБ:

$$К_{опт} = \sum П_i \qquad (2.5)$$

$К_{опт}$ – коэффициент оптимальности;

$П_i$ – показатель оптимальности для i ИСБ:

$$П_i = К_{вес} \times П_{хар} \qquad (2.6)$$

$К_{вес}$ – обобщенный весовой коэффициент n характеристики;

$П_{хар}$ – нормированные параметры n характеристики для i ИСБ.

Нормированные параметры n-ой характеристики для i-ой интегрированной системы безопасности ($П_{хар}$) можно посмотреть в таблице приложения 3. Где 1 балл присваивается наибольшему параметру, остальные значения рассчитываются через пропорции, относительно наибольшего параметра.

В результате вычислений получили следующие показатели коэффициента оптимальности, представленные в таблице 2.3.

Таблица 2.3.

Коэффициенты оптимальности интегрированных систем безопасности.

№ п/п	Название ИСБ	Значение коэффициента оптимальности
1.	Кодос А-20	5,94
2.	Ладога-А	4,28
3.	Пахра	8,46
4.	Рубеж-08	8,28
5.	Стрелец-Интеграл	5,43

Исходя из полученных оценок, выберем интегрированную систему безопасности «Пахра», так как именно она получила наивысшую оценку. Следует отметить также интегрированную систему безопасности «Рубеж-08» которой не хватило нескольких десятых баллов до ИСБ «Пахра». Тем не менее, ее можно было бы использовать в проектировании системы безопасности.

ГЛАВА 3. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО ПОСТРОЕНИЮ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЪЕКТА ОФИСНОГО ЗДАНИЯ

3.1. Система охранно-тревожной сигнализации и контроля и управления доступом

Для построения комплексной системы безопасности (КСБ) объекта электроэнергетики применена программная платформа «SecurOS», производства компании ISS (данная платформа используется также и для организации видеосервера), которая позволяет интегрировать оборудование и программное обеспечение различных производителей. Таким образом, платформа «SecurOS» обеспечивает создание единого интерфейса, настройки логики работы и сценариев взаимодействия подсистем контроля и управления доступом, охранно-тревожной сигнализации и охранной телевизионной. Связь видеосервера, охранно-тревожной сигнализаций, контроля и управления доступом осуществляется по интерфейсному кабелю – витой паре 5 категории. Также возможно модульное и функциональное наращивание КСБ, в том числе интеграция других подсистем безопасности при необходимости, например пожарной сигнализации.

Основными задачами разработанной системы охранной сигнализации, контроля и управления доступом являются:

- защита жизни, здоровья лиц находящихся на территории объекта при возникновении чрезвычайных ситуаций;
- защита материальных и информационных ценностей, находящихся в помещении;
- защита собственных ресурсов, систем и технических средств, при попытках несанкционированного доступа к ним, контроль работоспособности комплекса (системы);

- обеспечение санкционированного входа в здание и в зоны ограниченного доступа и выход из них путем идентификации личности по комбинации различных признаков: вещественный код (виганд-карточки);
- предотвращение несанкционированного прохода в помещения и зоны ограниченного доступа объекта.

Исходя из характеристик объекта, эксплуатационных требований и технического задания на проектирование, в работе предусматривается создание систем охранной сигнализации, контроля и управления доступом на основе оборудования НВП «Болид» (г. Королев). Основой построения системы является пульт контроля и управления «С2000-М» (далее – пульт). Пульт предназначен для работы в составе систем охранной сигнализации, контроля и управления доступом, а также контроля состояния и сбора информации с приборов системы, ведения протокола возникающих в системе событий, индикации тревог, управления постановкой на охрану (снятием с охраны), управления автоматикой. Приборы (контроллер С2000-2) и пульт объединяются в систему по интерфейсу RS-485. В системе пульт выполняет функцию центрального контроллера, собирающего информацию с подключенных приборов и управляющего взятием/снятием шлейфов сигнализации (ШС) приборов и системными выходами (релейными выходами или выходами «открытый коллектор»). При поступлении извещения о пожаре, пульт С2000-М, дает команду на заранее запрограммированные контроллеры С2000-2, о разблокировке точек прохода.

Для управления доступом, через одну или две точки доступа, путем считывания кодов через считыватель «Proxy-3A», также для проверки прав доступа и управления запорными устройствами (электромеханическими и электромагнитными замками и защелками, турникетом) посредством замыкания (размыкания) контактов реле – используется контроллер доступа «С2000-2» (далее контроллер). Контроллер обеспечивает анализ состояния двух охранных шлейфов сигнализации (ШС) с управлением

постановкой/снятием ШС с охраны при помощи Proximity-карт и по интерфейсу RS-485. Если в момент формирования сообщения контроллер не имел связи с сетевым контроллером, то событие будет храниться в энергонезависимом буфере, и при восстановлении связи по интерфейсу RS-485, будет передано в сетевой контроллер с указанием времени и даты его возникновения, что позволяет «С2000-2» работать автономно с сохранением все прав доступа.

Данные с контроллеров по интерфейсу RS485 поступают на «С2000-ПИ», далее на пульт «С2000-М», с последующей передачей на сервер интегрированной системы безопасности установленный в помещение серверной на первом этаже (помещение 14), далее информация через коммутатор (Cisco Catalyst 2940-8TT) поступает в помещение охраны, с установленным программным обеспечением и разными правами доступа. Пульт «С2000-М» обеспечивает дополнительное резервирование событий системы в случае неисправности компьютера. Передача тревожных сообщений осуществляется на ПЦН.

Для контроля состояния помещений, охранной сигнализации используются:

– приемник радиоканальный «РПУ Астра-РИ-М»;
– кнопка тревоги беспроводная «РПДК Астра-РИ-М»;
– извещатель охранный объемный «Астра-5;
– извещатель охранный звуковой «Астра-С»;
– извещатель магнито-контактный «ИО-102-4» и «ИО-102-26»;
– кнопка тревожной сигнализации «ИО 101-1(А)».

Для контроля и управления доступом в помещения используются:

– считыватель «Proxy-3A»;
– электромагнитный замок врезной «AL-300 SHG»;
– электромагнитный замок выносной «AL-300»;
– кнопка выхода пластиковая «EX-01»;
– контроллеры доступа «С 2000-2».

Резервирование электропитания контроллеров осуществляется от источников бесперебойного питания «Скат 1200М» с выходным напряжением 12В, установленных в охраняемых помещениях.

Основные эксплуатационные возможности, технические характеристики и инструкции по эксплуатации использованного оборудования: пульта контроля и управления ПКУ «С2000-М», приемника радиоканального «РПУ Астра-РИ-М», кнопки тревоги беспроводной «РПДК Астра-РИ-М», извещателя охранного объемного «Астра-5; извещателя охранного звукового «Астра-С», извещателя магнито-контактного «ИО-102-4» и «ИО-102-20», кнопки тревожной сигнализации «ИО 101-1(А)», считывателя «Proxy-3A», электромагнитного замка врезного «AL-300 SHG», электромагнитного замка выносного «AL-300», турникета электромеханического «Т-283», кнопки выхода «EX-01», контроллера доступа «С 2000-2», коммутатора (Cisco Catalyst 2940-8TT) и др.приведены в технической документации на сайтах фирм-разработчиков и предприятий изготовителей, а также на сайте компании «Тинко».

Оборудование систем охранно-тревожной сигнализации, контроля и управления доступом устанавливается внутри охраняемого здания объекта на высоте 1,4-1,6м от пола. Прокладка шлейфов сигнализации производиться скрыто, за подвесным потолком, кабелем КСПВ 2*0,4 и 4*0,4 слаботочной части, шнуром ШВВП 2*0,75 низковольтной сети электропитания. Линия интерфейса RS-485 выполняется кабелем КПКЭВнг FRLS 1х2х0,75. Электропитание «Скат 1200М» осуществляется напряжением 220В кабелем ВВГнг 3х2,5 проложенным за подвесным потолком в гофрированной ПВХ трубе Ду25, идущим от автоматических выключателей 6А, установленных в распределительном щите системы безопасности (ЩР1). Распределительный щит включает шесть групп электропотребителей: первая и вторая группа (первый этаж); третья группа (второй этаж); четвертая группа (третий этаж); пятая группа (мансардный этаж); шестая группа (первый этаж, помещение охраны). Через

строительные конструкции шлейфы сигнализации прокладываются в жесткой ПВХ трубе Ду32. Разводка кабелей выполнена на расстоянии не менее 0,5м от силовых кабелей, 0,25м от осветительных приборов. Кабель промаркирован с двух сторон, на ответвлениях, в коммутационных коробках – в соответствии с нумерацией в кабельном журнале (в обозначении первая цифра – номер прибора, вторая – номер кабеля, третья – номер извещателя). В местах, где отсутствует возможность скрытой прокладки кабельных трасс используется нераспространяющий горение электротехнический пластиковый короб. Сечение пластиковых коробов обеспечивает возможность прокладки дополнительных проводов и кабелей с целью наращивания структуры сигнализации и контроля доступа.

Монтаж выполняется с минимальным нарушением интерьера помещений и должен соответствовать техническим и эргономическим нормам. Монтаж оборудования производится квалифицированным персоналом, имеющим допуск для проведения работ с электрооборудованием до 1000 В в соответствии с технической документацией производителя и действующими нормами, и правилами по монтажу оборудования слаботочных сетей.

Конфигурация систем и применяемое оборудование обеспечивают возможность наращивания за счет расширения аппаратной части и монтажа дополнительных извещателей без нарушения работоспособности смонтированного комплекса.

Комплект разработанных чертежей на системы охранно-тревожной сигнализации, контроля и управления доступом приведен в приложении Б выпускной квалификационной работы.

Резервирование электропитания контроллеров осуществляется от источников бесперебойного питания «Скат 1200М» с выходным напряжением 12 В, установленных в охраняемых помещениях.

3.2. Система охранная телевизионная

Средствами охранными телевизионными оборудуются все четыре этажа административного здания, а также периметр территории объекта электроэнергетики.

Система охранная телевизионная (СОТ) предназначена для визуального наблюдения, контроля и регистрации видеоинформации с целью дальнейшего просмотра и анализа охраняемых зон объекта.

СОТ обеспечивает:

– передачу визуальной информации о состоянии помещений в здании, периметра и территории объекта в помещение охраны;

– многоканальную видеозапись (высокую скорость, индивидуальную настройку параметров, настройки режима записи, программная обработка и улучшение качества изображения);

– отображение и воспроизведение (цифровое увеличение, настройки контраста, цветности, четкости, многоэкранное представление записи, удаленный просмотр, одновременное отображение, запись и просмотр видеоинформации);

– формирование видеоархива (большой объем, возможность сжатия без потерь в качестве, мгновенный поиск записи по признаку места и времени, события, номеру камеры, покадровый и ускоренный просмотр).

Программная платформа «SecurOS» производства компании ISS позволяет интегрировать оборудование и программное обеспечение различных производителей.

Таким образом платформа «SecurOS» обеспечивает создание единого интерфейса, настройки логики работы и сценариев взаимодействия видеоподсистемы, системы контроля и управления доступом, и охранно-тревожной сигнализации.

Основой построения СОТ Hi-Live IV – 40 является плата видеозахвата TV ISS4E в количестве 2 штук и плата видеозахвата TV ISS4

в количестве 2 штук на базе программного обеспечения «SecurOS». Скорость обработки видеосигнала 280 кадров в секунду. Общее количество каналов – 40. Данная система имеет возможность дальнейшего расширения до 40 видеокамер.

Запись со всех видеокамер наблюдения ведется на жесткий магнитный диск. Сигналы от видеокамер поступают на видеосервер, который устанавливается в серверном зале на первом этаже, далее информация через коммутатор (Cisco Catalyst 2940-8TT) – предусмотренный проектом поступает в помещение охраны, отдела кадров и СЭПАК, с установленным программным обеспечением и разными правами доступа.

С поста охраны имеется возможность просмотра картинок изображения со всех 32 камер и управления полноприводными камерами вручную.

Для наружного наблюдения используются 3 типа видеокамер.

По периметру расставлены цветные видеокамеры Smartec STC-3640/3 в количестве 8 штук (AS1-AS7,AS10). Также данный тип камер используется в помещениях 14 и 12 (AS12, AS13)

Технические характеристики камеры Smartec STC-3640/3 приведены в табл. 3.1.

Таблица 3.1

Технические характеристики камеры Smartec STC-3640/3

№ п/п	Наименование параметра	Значение параметра
1.	Тип камеры:	«День/ночь»
2.	Чувствительный элемент:	1/3” цветная ПЗС Sony SuperHAD
3.	Количество пикселей:	752 x 582

Для контроля территории у центрального входа в здание используются цветные камеры Smartec STC-3650/3 XTREEM (AS8, AS9)

Для полного контроля прилегающей к центральной и боковой частям фасада территории используются полноприводные цветные видеокамеры Panasonic WV-CW964 (AV1, AV2), имеющие следующие характеристики (см. табл. 3.3). Технические характеристики камеры Smartec STC-3650/3 приведены в табл. 3.2. Основой построения СОТ Hi-Live IV – 40 является плата видеозахвата TV ISS4E в количестве 2 штук и плата видеозахвата TV ISS4 в количестве 2 штук на базе программного обеспечения «SecurOS». Скорость обработки видеосигнала 280 кадров в секунду. Общее количество каналов – 40. Данная система имеет возможность дальнейшего расширения до 40 видеокамер.

Таблица 3.2

Технические характеристики камеры Panasonic WV-CW964

№ п/п	Наименование параметра	Значение параметра
1.	Разрешающая способность	752 (г.) x 582 (в.), 1/4-дюймовая ПЗС матрица со встроенной функцией Super Dynamic III
2.	Область сканирования	3.65 мм - 2.71 мм
3.	Выходной видеосигнал PAL,	композитный CCIR
4.	Синхронизация	Внутренняя / Внешняя / VD2
5.	Развертка	2:1 чересстрочная
6.	Частота горизонтальной развертки	15,625 кГц
7.	Частота вертикальной развертки	50,0 Гц
8.	Выходной видеосигнал	VBS: 1,0 В (амплитуда) / 75 Ом / BNC разъем
9.	Разрешающая способность	Горизонтальное: мин. 480 ТВ строк (цветной нормальный режим 540 ТВ строк (обычно), мин. 520 ТВ строк (цветной качественный режим, минимум

№ п/п	Наименование параметра	Значение параметра
		570 ТВстрок- (чернобелый) Вертикальное: минимум 400 ТВ строк (среднее)
10.	Минимальная освещенность	0,5 люкс (цветной режим) 0,04 люкс (черно-белый режим) увеличение чувствительности: откл.; ару: выс. уровень
11.	Отношение сигнал/шум	54 дБ в среднем («Super Dynamic III»: ВКЛ.); Минимум 50 дБ (АРУ: ОТКЛ.)
12.	Диапазон поворота	360° - бесконечность
13.	Скорость поворота	Ручной: около 0,065 °/сек ~ 120 °/сек 8 - шаговая, 16 - шаговая, 64 - шаговая. По предустановкам: около 400 °/сек
14.	Диапазон наклона	-5 °~ 185 °(горизонтально - вертикально - горизонтально) (В соответствии с параметром «угол наклона»)
15.	Скорость наклона	Ручной режим: около 0,065 - 120° /сек., 8 - шаговая, 16 - шаговая, 64 - шаговая. По предустановкам: 400°/сек.
16.	Кратность масштабирования	х 300 (х30 оптическое плюс цифровое масштабирование х10)
17.	Фокусное расстояние	3.8 - 114 мм

№ п/п	Наименование параметра	Значение параметра
18.	Макс. апертура объектива	F1.4 (широкий) - 3.7 (теле)
19.	Минимальное расстояние до объекта	1,5 м
20.	Диапазон ирисовой диафрагмы	F1.4 - 22, закрыта
21.	Угол поля зрения	по гортзонтали 1,9° - 52°, по вертикали 1,4° - 40°
22.	Контроллер интерфейса	Мультиплексно-коаксиальный / RS-485
23.	Управление	Поворот/наклон, объектив, 256 предустановленных положения, базовая настройка, патрулирование
24.	Автоуправление усилением	(AGC) Вкл. (низкий) / вкл (средний) / вкл. (высокий) / выкл.
25.	Идентификация камеры	Предустановленная идентификация (ID}, ID камеры, название области до 16 символов
26.	Скорость фокусирования	Около 6,0 с (вдали / вблизи) в ручном режиме
27.	Защита паролем	Все настройки
28.	IRIS диафрагма	Автоматическая (открыта / закрыта / ручной режим)
29.	Электронный затвор (сек.)	1/50 (выкл.), 1/120, 1/250, 1/500, 1/1000,1/2000, 1/4000, 1/10000 с
30.	Чувствительность	Max. повышение в 32 раза, авто./фикс.
31.	Автоматический режим	Выкл. / последовательный / сортировка / автоповорот / патрулирование

№ п/п	Наименование параметра	Значение параметра
32.	Super Dynamic III	(Вкл./Выкл.)
33.	Цифровой переворот	Вкл./Выкл.
34.	Детектор движения	Выкл./Установка1 /Установка2
35.	Ч/б режим	Авто /вкл. /выкл.
36.	Зона секретности	Вкл./Выкл., до 8 зон
37.	Патрулирование	Стоп / Воспроизведение / Обучение
38.	Удержание изображения	Вкл./Выкл.
39.	Температура окр. среды	От -40° до +50°С
40.	Влажность окр. среды	менее 90% (без конденсации)
41.	Источник питания	24 В перм. тока 50 Гц
42.	Потр. Мощность	77 Вт
43.	Размеры (диаметр х высота)	239 мм х 395 мм
44.	Вес	около 4,7 кг.

Для внутреннего наблюдения используются цветные видеокамеры Ai-DC59 в количестве 18 штук (AS11, AS14-AS30). Данная камера имеет следующие характеристики (см. табл. 3.4).

Таблица 3.4

Технические характеристики камеры Ai-DC59

№ п/п	Наименование параметра	Значение параметра
1.	Стандарт видеосигнала	PAL
2.	ПЗС-матрица	1/3" SONY Super HAD CCD
3.	Разрешение	600 ТВЛ
4.	Размер изображения	795 × 596
5.	Объектив	Стандартно : f2,9мм-10мм/F1,2 асферический с автодиафрагмой

		/74,2°~30,0°
6.	Объектив	Дополнительно : f2,5мм-6,0мм/F1,3 асферический с автодиафрагмой /108,2°~47,6° f9,0мм-22,0мм/F2,0 автодиафрагма /29,2°~13,0°
7.	Минимальная чувствительность	0,25 Люкс / F1,2
8.	Сигнал/шум	До 50 дБ (АРУ выкл.)
9.	Автоматическая регулировка усиления	Вкл./выкл.
10.	Синхронизация	Встроенная
11.	Автоматический электронный затвор	Вкл./выкл.
12.	Компенсация заднего освещения	Вкл./выкл.
13.	Устранение мерцания	Вкл./выкл.
14.	Баланс белого	Автоматическое отслеживание белого
15.	Видеосигнал	1,0 Vp-p композитный / 75 Ом (BNC-коннектор)
16.	Потребляемая мощность	2 Вт
17.	Рабочая температура	от -30 до +50 °C
18.	Влажность	до 85 %
19.	Размеры	118 × 88 мм
20.	Вес	12 В: 300 г 12 В/24 В: 370 г

Крепление камер производится в соответствии с паспортом оборудования.

Крепление наружных камер осуществляется на высоте примерно 4 м. Крепление наружных камеры AV2 осуществляется на высоте примерно 15 м. Крепление внутренних камер осуществляется на потолок.

Монтаж оборудования СОТ проводится квалифицированным персоналом в соответствии с технической документацией производителя и действующими нормами, и правилами по монтажу оборудования

слаботочных сетей. Монтаж системы производится скрыто в запотолочном пространстве.

Монтаж кабельных сетей внутри здания производится скрыто с использованием не распространяющего горения электротехнического пластикового короба, нейлоновых стяжек и лотков. Снаружи здания с использованием трубы гофрированной сечением, соответствующим прокладываемому кабелю.

Сечение пластиковых коробов обеспечивает возможность прокладки дополнительных проводов и кабелей с целью наращивания системы телевизионного охранного наблюдения.

Монтаж должен быть выполнен с минимальным нарушением интерьера помещений и должен соответствовать техническим и эргономическим нормам.

3.3. Выполнение требований по технике безопасности и охране труда при выполнении работ по внедрению комплексной системы безопасности

Государственные нормативные требования охраны труда обязательны для исполнения юридическими и физическими лицами при осуществлении ими любых видов деятельности (ст. 211 ТК РФ)

Пунктом 3 статьи 37 Конституции РФ установлено право каждого на труд в условиях, отвечающих требованиям безопасности и гигиены. В соответствии с положениями статьи 209 Трудового кодекса, под охраной труда подразумевается система сохранения жизни и здоровья работников в процессе трудовой деятельности.

Выполнение правил по охране труда обязательно как для работодателя, так и для работников организации

Требования по охране труда, промсанитарии и технике безопасности обеспечиваются следующими проектными решениями:

– размещение оборудования в помещении производится таким образом, чтобы получить свободный доступ к нему при монтаже и эксплуатации;

– ограждение токонесущих частей и блоков оборудования, находящихся на доступной высоте;

– применение быстродействующих автоматических выключателей;

– устройством заземления металлических частей оборудования нормально ненаходящихся под напряжением, но которые могут оказаться под напряжением в результате аварии в электрических цепях.

Оборудование, входящее в состав КСБ, не выделяет вредных веществ и выбросов в окружающую среду.

Устанавливаемое по проекту оборудование соответствует правилам электропожаробезопасности, а по уровню шума санитарным нормам и правилам.

Таким образом, в настоящем разделе приведены основные технические решения по построению систем охранно-тревожной, сигнализации, контроля и управления доступом и охранной телевизионной офисного здания, в том числе разработан соответствующий комплект чертежей: структурные схемы, спецификации оборудования и материалов подсистем.

ГЛАВА 4. КОМПЛЕКСНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

4.1. Определение, задачи и функциональные возможности комплексных систем безопасности

Комплексные системы безопасности объединяют в себе множество различных систем (подсистем) и обеспечивают более надежную

безопасность на объектах и прилегающих территориях. Причем безопасность достигается целым комплексом мер. Одной из них является выявлением угроз и их нейтрализация с помощью интегрированных систем безопасности (ИСБ). ИСБ подходят для любого объекта. Неважно что это будет завод или промышленные предприятие, морской порт или аэродром, торговая точка или образовательное учреждение, ИСБ успешно справятся с задачей по обеспечению безопасности на объекте путем:

- осуществления на охраняемых объектах (здания, помещения, территории, зоны) контроля и управления доступом персонала и посетителей;
- обнаружения на охраняемых объектах несанкционированного проникновения;
- обнаружения на объектах охраны несанкционированных действий.

Для организации пропускного режима в организациях устанавливаются системы контроля и управления доступом (СКУД), так же СКУД разграничивает доступ в конкретные помещения если это требуется. Охранно-пожарная сигнализация (ОПС) занимается выявлением признаков пожара, несанкционированного доступа на объекте. А система охранного телевидения (СОТ) позволяет визуализировать происходящее событие, замеченное ОПС.

Благодаря СКУД, независимо от величины охраняемого объекта, можно сократить расходы на обычную охрану. СКУД может ограничивать доступ как в целом на объект, так и в отдельные его помещения (например, складские помещения, сейфы и т.п.). СКУД состоит из:

– пропускной системы или устройства ввода идентификационных признаков;
– ограждающих устройств (шлагбаумы, турникеты, шлюзовые

кабины и т.д.);

– устройств управления, защищенное от несанкционированного доступа.

СКУД необходимо оборудовать главные и служебные входы, КПП, помещения, в которых хранятся товарно-материальные ценности и другие не менее важные помещения. При этом общий допуск на территорию объекта может осуществляться по одному признаку, а доступ в другие зоны по другому признаку или даже группе признаков.

СОТ, как уже было сказано ранее, позволяет следить за обстановкой на объекте. В случае получения извещения о нарушении ШС именно видеонаблюдение позволяет определить характер и место нарушения и принять оптимальные меры.

СОТ состоит из:

– телевизионной камеры;

– видеомонитора;

– источника электропитания;

– линии передачи.

СОТ обязательно размещается у главного и служебного входов в здания, на КПП для идентификации проходящих лиц, на периметре охраняемого объекта, в помещениях, где хранятся материальные ценности и в коридорах, по которым происходит перемещение материальных ценностей. К камерам, размещенным в разных точках, предъявляются разные требования. Например, камеры на улицах должны иметь герметичные термокожухи, козырьки, защищающие от солнца, и должны быть поставлены так, чтобы лучи солнца не попадали в объектив.

Охранную сигнализацию можно разделить на: периметральную и внутриобъектовую. При установке сигнализации по периметру нужно

учесть рельеф местности, предполагаемые угрозы, тип ограждения, зона отторжения, помеховая обстановка, протяженность территории и ее укрепленность.

А для защиты внутренних помещений необходимо устанавливать сигнализацию в зонах, где хранятся и по которым перемещаются материальные ценности, а также в уязвимых местах, к которым относятся окна, двери, вентиляционные шахты.

Помимо ОПС по мере необходимости подключают тревожную сигнализацию. Она активируется при помощи человека путем нажатия на

«Тревожную кнопку», которая устанавливается в хранилищах, сейфах, в кабинете бухгалтера и руководителя, на постах охраны, у всех входов в здание. Тревожная сигнализация может быть ручной и ножной и должна размещаться в незаметных обычным посетителям местах.

Пожарная сигнализация нужна для обнаружения очагов возгорания и оповещение о пожаре на объекте. В зависимости от предполагаемой угрозы подключают дымовые, тепловые, дифференциальные, аспирационные извещатели, извещатели обнаружения пламени. Соответственно, каждый из них срабатывает при появлении характерного признака. Для повышения точности и надежности обнаружения признаков пожара рекомендуется использовать комбинированные пожарные извещатели.

Так же не стоит забывать о системе оповещения. Она присутствует в каждой подсистеме (системе) безопасности в виде световых и звуковых оповещателей, световых табло и т.д. Однако в ряде случаев система оповещения может представлять собой отдельную систему, например, систему речевого оповещения.

Перед системой оповещения ставится задача по информированию сотрудников объекта о возникшей нештатной ситуации на объекте и осуществлять координацию их действий по выполнению эвакуации с опасного объекта.

Технических систем безопасности большое множество и каждая решает свои определенные задачи. Поэтому эффективнее всего использовать комплексный подход, обеспечивая целый комплекс мер. Важно организовать защиту и контроль на всех уровнях, и комплексный подход позволяет сделать это максимально эффективно.

Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений и объектовым техническим средствам охраны, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» от 28.04.2018 г. определяет перечень систем безопасности рекомендуемых для применения на объектах охраняемых подразделениями вневедомственной охраны. К таким системам относятся: «Кодос А-20», «Ладога-А» (с дополнительным оборудованием), «Пахра», «Рубеж-08», «Стрелец Интеграл».

Рассмотрим более подробно назначение, технические характеристики и особенности таких систем.

Охранную сигнализацию можно разделить на: периметральную и внутриобъектовую. При установке сигнализации по периметру нужно учесть рельеф местности, предполагаемые угрозы, тип ограждения, зона отторжения, помеховая обстановка, протяженность территории и ее укрепленность.

4.2. Система безопасности на базе прибора приемно-контрольного охранно-пожарного «Кодос А-20»

Интегрированная система безопасности на базе прибора приемно-контрольного охранно-пожарного «КОДОС А-20» предназначена для обнаружения и идентификации нарушителя на охраняемом объекте, подачи извещения о тревоге на автоматизированное рабочее место и предоставление в удобном виде информации о нарушителе, а также для

обнаружения пожара и подачи извещения о тревоге. После чего принимается комплекс мер по задержанию нарушителя или устранение пожара. К основным функциям системы охранно-пожарной сигнализации на базе ППКОП «Кодос-А20» относят:

– регистрация, обработка и передача на пульт централизованного наблюдения (ПЦН) информации от шлейфов сигнализации (ШС);

– управление по заданным алгоритмам исполнительными устройствами систем пожаротушения и дымоудаления, а также оповещения и эвакуации;

– формирование управляющих сигналов для других систем безопасности.

Система осуществляет контроль четырех состояний («Норма», «Тревога», «Короткое замыкание» и «Обрыв») как пожарных, так и охранных шлейфов, которые, в свою очередь, контролируют от одного до нескольких датчиков, в зависимости от пожарных норм и их токопотребления, управление по заданным алгоритмам исполнительными устройствами систем пожаротушения и дымоудаления, а также оповещения и эвакуации;

В таблице 2.1 приведены технические данные прибора приемно-контрольного охранно-пожарного КОДОС А-20.

Таблица 4.1.

Основные технические данные прибора А-20

№ п/п	Характеристика	Значение
1.	Напряжение питания, В	9,5 … 15,0
2.	Ток потребления, А	не более 3
3.	Число подключаемых к прибору считывателей «КОДОС-RD», шт	2
4.	Длина линии связи от прибора до считывателя, м	не более 30
5.	Число подключаемых к прибору модулей индикации «МИ-50», шт	не более 8

6.	Длина линии связи от прибора до модуля индикации «МИ-50», м	1200
7.	Ток потребления сирены №1, сирены №2, А	не более 1
8.	Напряжение питания сирены №1, сирены №2, В	не более 12,0
9.	Максимальное число паролей пользователей, карт пользователей, вариантов групповой постановки извещателей на охрану	256

4.3. Интегрированный комплекс технических средств охраны «Пахра»

«Пахра» – это интегрированный комплекс безопасности (ИКБ), предназначенный для обеспечения комплексной безопасности зданий, сооружений, внутренней территории и периметров объектов средней и большой величины.

Интегрированный комплекс безопасности «Пахра» работает под управлением фирменного программного обеспечения КСА ПЦО

«Радиосеть», разработанного на основе использования единой информационной модели для всех входящих в интегрированный комплекс безопасности «Пахра» подсистем.

Интегрированный комплекс безопасности «Пахра» разработан с использование следующих принципов:

– сотовая структура;

– интеграция на всех уровнях;

– цифровые способы сбора и обработки данных.

В сотовом принципе построения объект охраны разбивается на отдельные локальные участки («соты») двух типов – линейные (периметры, ограждения и пр.) протяженностью до 600 метров и пространственно- распределенные (производственные и служебные помещения, ангары и др.) площадью до квадратного километра. Общее количество сот в системе не ограничено.

Безопасность соты, в зависимости от ее типа, обеспечивают специальные устройства – сервер локального участка периметра (СЛУП) или сервер локальной зоны (СЛЗ) с подключённым к ним периферийным оборудованием. Каждый сервер интегрирует в себе функции охранной и тревожной сигнализации, контроля и управления доступом, охранного телевидения, речевой связи и оповещения. Серверы служат также устройствами ретрансляции информации со смежных сот на пульт централизованного наблюдения и обратно.

Разбиение объекта охраны на локальные зоны позволяет уменьшить длину линий связи с удаленными периферийными устройствами за счёт подключения их к серверам.

Тактико-технические характеристики сервера интегрированной системы безопасности «Пахра» приведены в таблице 2.3.

В сотовом принципе построения объект охраны разбивается на отдельные локальные участки («соты») двух типов – линейные (периметры, ограждения и пр.).

Таблица 2.3.

Тактико-технические характеристики сервера ИСБ «Пахра»

№ п/п	Характеристика	Значение
1.	Количество приборов приемно-контрольных охранно-пожарных на 5 шлейфов сигнализации с функциями двухсторонней речевой связи и оповещения, контроля и управления одной точкой доступа	до 480 шт.

2.	Количество устройств двухсторонней речевой связи с функциями тревожной сигнализации и контроля наряда.	до 12 шт.
3.	Количество устройств речевого оповещения по громкой связи	до 4 шт.
4.	Количество видеокамер	до 12 шт.
5.	Кадровая частота.	25 кадров/сек на канал
6.	Разрешение видеокамер	704x576
7.	Потребляемая мощность	до 300 Вт.

4.4. Интегрированная система безопасности «Рубеж-08»

ИСБ состоящая из ППКОП «Р-08» и дополнительного оборудования, предназначена для создания интегрированных систем безопасности средних и крупных объектов, в состав которых входят подсистемы: охранной сигнализации (ОС), тревожной сигнализации (ТС), пожарной сигнализации (ПС), технологической сигнализации, системы контроля и управления доступом (СКУД), управления исполнительными устройствами и другие.

Аппаратная интеграция подсистем на уровне оборудования и независимость работы от ПК обеспечивают высокую эффективность и надежность функционирования системы безопасности. Технические характеристики БЦП «Рубеж-08» представлены в таблице 2.4

Таблица 2.4.

Технические характеристики БЦП «Рубеж-08»

№ п/п	Характеристика	Значение
1.	Средняя наработка на отказ БЦП	Не менее 1800 ч.
2.	Средний срок службы прибора	10 лет
3.	Диапазон рабочих температур	От -50 ℃ до +50 ℃

4.	Сеть постоянного тока или резервного источника	10,5…28 В
5.	Ток нагрузки	1 А
6.	Мощность потребления	Не более 60 Вт
7.	Количество встроенных ШС БЦП	8

4.5. Интегрированная система безопасности «Стрелец-Интеграл»

Интегрированная система безопасности Стрелец-Интеграл – это: беспроводная и проводная охранная сигнализация, которая предназначена для обеспечения безопасности на различных объектах большой и средней протяженности.

Интегрированная система безопасности Стрелец-Интеграл обладает большими возможностями по интегрированию беспроводных устройств предыдущего поколения системы Стрелец и проводных устройств системы нового поколения. Интегрированная система безопасности Стрелец- Интеграл состоит из множества сегментов. Одним сегментом можно обозначить отдельное здание или группу этажей в здании. В системе Стрелец-Интеграл устранены недостатки систем предыдущего поколения и учтены преимущества. ИСБ стала значительно надежнее (помехоустойчивость, живучесть) и позволяет использовать её для контроля безопасности коммерческих объектов, социальных и особо значимых объектов, оперативного управления пожаротушением и оповещением при пожарах и других чрезвычайных ситуациях. Оборудование ИСБ обеспечивает единообразный централизованный контроль радиоканальных и проводных (адресных и неадресных) извещателей и управление радиоканальными и проводными исполнительными устройствами. По классификации ГОСТ Р 53325 в части технических средств пожарной автоматики ИСБ представляет

собой прибор приёмно-контрольный и управления пожарный (ППКП) со следующими характеристиками:

Емкость системы:

– 255 сегментов в системе;

– 127 приборов в сегменте (например, РРОП–И или БШС8–И);

– 1920 адресов в сегменте (например, извещателей или шлейфов).

Для системы Стрелец-Интеграл разработан набор специализированных объектовых устройств, подключаемых к объектовой системе по протоколу LonWorks, обеспечивающие автоматический мониторинг по: GSM/GPRS; Contact ID; IP-сетям; радиоканалу (150 МГц, 25мВт; 146-174 МГц, 5 Вт; 403-470 МГц, 5 Вт). В состав ИСБ входит набор устройств, состав и количество которых определяется при заказе с учётом характеристик объекта с учётом требуемых функций

Интегрированных системы безопасности очень много и все они прекрасно справляются со своей задачей по осуществлению надежной охраны объектов, но у каждой системы есть свои недостатки и преимущества. Именно поэтому необходимо выявить для проектного задания наиболее подходящую систему безопасности.

ГЛАВА 5. РАСЧЕТ ТЕХНИЧЕСКИХ ПАРАМЕТРОВ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ОФИСНОГО ЗДАНИЯ

5.1. Расчет электропитания систем охранно-тревожной сигнализации и контроля и управления доступом

Основные требования к электропитанию подсистем ИСБ изложены в соответствующих нормативно-технических документах.

Основное электропитание подсистем ИСБ должно осуществляться от сети переменного тока частотой 50 Гц с номинальным напряжением 220 В по первой категории надежности согласно ПУЭ.

Все токопроводящие части оборудования нужно заземлить с использованием общего контура существующего заземления объекта. Защитное заземление оборудования осуществляется от заземляющих устройств, имеющих сопротивление не более 4 Ом.

Для исключения сбоев в работе подсистем ИСБ при отключении электропитания общей сети ~220В должна быть предусмотрена система резервного питания, состоящая из химического источника электрического тока (свинцово-кислотной аккумуляторной батареи), который устанавливается в корпус источников бесперебойного питания для обеспечения автономной работы подсистем.

Емкость аккумуляторной батареи рассчитывается по следующей формуле: $C_{АКБ} = 1.3 \times I_{сум} \times t$, где $C_{АКБ}$ — емкость батареи; $I_{сум}$ — суммарный ток; t — время работы системы от резервного источника; 1.3 — 30% запас емкости АКБ, необходимый для предотвращения полного разряда аккумуляторной батареи.

Подачу электропитания к приборам необходимо производить от свободной группы щита аварийного (эвакуационного) освещения, а при его отсутствии – от щита дежурного освещения непосредственно от отдельной группы, без промежуточных выключателей.

При отсутствии на электрощитах свободной группы подключение проводов питания производят от вводных клемм с установкой электрощита с плавкими предохранителями или вставками у прибора.

Примеры расчета бесперебойного электропитания подсистем ИСБ рассматриваются в.

Выбор блока питания зависит от рода, номинального напряжения и тока, необходимого для нормальной работы приборов.

Максимальная общая нагрузка на один источник:

– контроллер доступа «С2000-2» - 1 шт;

– замок электромагнитный «AL – 300» – 2 шт;

– считыватель «Proxy-3A» - 2шт;

– извещатель охранный объемный «Астра-5» - 3шт;

– извещатель охранный объемный «Астра-С» - 3шт.

Ток потребления приборов:

– «С2000-2» - 120мА;

– «AL – 120» - 350 мА;

– «Proxy-3A» - 120 мА;

– «Астра-5» - 12 мА;

– «Астра-С» - 12 мА.

Общий ток потребления приборов:

I = 120 + 700 + 240 + 36 + 36; I = 1132 (мА)

Напряжение питания всех потребляющих приборов 12В.

При прекращении энергоснабжения системы от основного источника, должен быть предусмотрен автоматический переход на функционирование от встроенного источника электропитания:

– 24 часа в дежурном режиме работы;

– не менее 3-х часов в режиме тревоги.

Допускается уменьшать время работы от резервного источника при наличии автоматического или иного оповещения подразделения вневедомственной охраны о моменте отключения основного электропитания в городах и поселках городского типа – до 4 часов в дежурном режиме и до 1 часа в режиме тревоги.

Минимальная емкость аккумулятора согласно этим требованиям рассчитывается следующим образом:

E = I x t x k/1000 , где:

E – емкость аккумулятора (Ач),

I – потребляемый ток (мА),

t – время работы от источника резервного питания (ч),

к – коэффициент аккумуляторной батареи.

E = 1132 x 4 x 1.3/1000

E = 5,9 Ач; т.е. минимальная емкость аккумулятора с учетом 30% запаса равна 7 Ач.

Выбираем для источника резервированного питания «СКАТ 1200М» аккумуляторную батарею емкостью 7 Ач.

Технические характеристики «СКАТ 1200М»:

– напряжение питающей сети: ~220В 50Гц с пределами изменения от 187 до 242В;

– температура окружающей среды от -10 до + 40˚С;

– номинальный ток нагрузки 1,7А;

– максимальный ток нагрузки при заряженной батареи 2,0А;

– максимальный ток нагрузки кратковременно (5 мин), 3,0А.

Технические средства охраны проектируемого комплекса обеспечивают свои характеристики при работе от однофазной электрической сети переменного тока напряжением 220В при колебаниях напряжения в пределах от +10 до -15%, и промышленной частоты 50 Гц +/- 1 Гц.

Обязательно выполняется заземление оборудования и устройств согласно ПУЭ и технической документации предприятий-изготовителей.

5.2. Расчет электропитания систем охранно-тревожной сигнализации и контроля и управления доступом

Трассы кабелей внутри здания проходят в коробах, в надпотолочном пространстве. Проход проводов и кабелей через стены и межэтажные перекрытия должен быть выполнен в твердой трубе ПВХ. Зазоры между проводом и трубой следует закладывать легко удаляемой массой из несгораемого материала (см. ГОСТР 50571.15-97 гл. 52). Трассы

снаружи здания проходят в гофрированной трубе соответствующего диаметра.

Электропитание внутренних и внешних видеокамер производится напряжением подводимым от блоков питания, установленных в помещении серверной; внешних стационарных камер от БП-3А (12В), внешних полноприводных камер от БП-24-5 (24В), внутренних видеокамер от Скат V.8 (12В).

Электроснабжение блоков вторичного питания осуществляется напряжением 220В кабелем ВВГнг 3х2,5, идущим от автоматического выключателя 6А, отдельного для каждого блока вторичного питания.

Электропитание сервера DSK и удаленного рабочего места DS осуществляется напряжением 220В кабелем ВВГнг 3х2,5, идущим от автоматического выключателя 16А. Все выключатели (16 шт – 6А, 2 шт – 16А) устанавливаются в электрическом щитке ШК. Электрический щиток ШК устанавливается на первом этаже в серверном зале.

Передача видеосигнала от внешних и внутренних камер до видеосервера и электропитание камер производится комбинированным кабелем РК75-3,7-35ф+2НВх0,5. Гарантированное электропитание электрического щитка ШК обеспечивает блок бесперебойного питания.

Блок бесперебойного питания должен обеспечивать выполнение основных функций системы при пропадании напряжений в сети на время равное не менее получаса.

Общая нагрузка на блок бесперебойного питания:

– блок вторичного питания БП-3А – 11 шт.
– блок вторичного питания СКАТ V.8 – 3 шт.
– блок вторичного питания БП-24-5 – 2 шт.
– сервер – 1 шт.
– удаленное рабочее место – 1 шт.

Ток потребления приборов:

– блок вторичного питания БП-3А – 0,125 А

– блок вторичного питания СКАТ V.8 – 0.3 А

– блок вторичного питания БП-24-5 – 0.8 А

– сервер – 4 А

– удаленное рабочее место – 7 А

Общий ток потребления приборов:

I = 11 х 0,125 +3х0.3 + 1.6 + 4 + 7 = 15 А

Общая нагрузка:

P= U x I,

P= 220 х 15 = 3300 ВА

Ввиду требования заказчика о необходимости двойного независимого резервирования сервера и всей системы видеонаблюдения выбираем два блока питания для установки в стойку APC Smart-UPS RT 5000 VA. Электропитание внутренних и внешних видеокамер производится напряжением подводимым от блоков питания, установленных в помещении серверной; внешних стационарных камер от БП-3А (12В), внешних полноприводных камер от БП-24-5 (24В), внутренних видеокамер от Скат V.8 (12В).

5.3. Расчет параметров сигнальной линии связи в комплексной системе безопасности

Для определения марки кабеля, соответствующей требованиям к передачи информации по протоколу RS-485 между сетевыми устройствами в разработанной комплексной системе безопасности объекта электроэнергетики необходим расчет первичных и вторичных параметров линии связи.

«Витая пара» в системе используется для объединения в единую сеть по протоколу RS-485 следующих устройств: приборы приемно-контрольные охранно-пожарные «Сигнал-20М», пульт контроля и управления «С2000-М», контроллеры доступа «С2000-2». Линия интерфейса RS-485 выполняется кабелем КИС-РПнг(А)-FRHF 2х2х0,80

Особенности.

Огнестойкий кабель КИС-РПнг(А)-FRHF 2х2х0,80 предназначен для одиночной и групповой прокладки в системах противопожарной защиты, охранно-пожарной сигнализации (ОПС), оповещения и управления эвакуацией людей при пожаре (СОУЭ), аварийного оповещения на путях эвакуации, аварийной вентиляции и противодымной защиты, автоматического пожаротушения, а так же в зданиях, сооружениях и строениях, где предъявляются требования к кабелям и проводам по сохранению работоспособности в условиях пожара (ГОСТ 53315-2009).

Конструкция кабеля КИС-РПнг(А)-FRHF 2х2х0,80 представляет собой комбинированное сочетание однопроволочных медных жил сечением 0,8 мм с изоляцией из органического кремния и полиолефинового слоя, скрутка – попарная, проводники в парах имеют цветовую кодировку, общий экран – алюмополимерная лента в оболочке из термопластичной безгалогенной композиции с дренажным проводником из медной луженой проволоки под экраном.

Условия эксплуатации:

Эксплуатируется внутри и вне помещений, при условии защиты от прямого солнечного излучения и атмосферных осадков. Вид климатического исполнения по ГОСТ 15150-69 — УХЛ категории размещения 2, 3, 4.

Класс пожарной опасности:

По ГОСТ Р 53315 «Кабельные изделия. Требования пожарной безопасности.» (П 1.1.2.2.2.) допускается применение кабеля в СОУЭ без использования негорючих коробов и кабельных каналов (в соответствии с письмом № 19-2-16-6542 от 23.10.2009 МЧС России).

Огнестойкие интерфейсные кабели, огнестойкая «витая пара» предназначены для одиночной и групповой прокладки в системах противопожарной защиты, в том числе системах охранно-пожарной сигнализации (ОПС), системах оповещения и управления эвакуацией

(СОУЭ), системах автоматического пожаротушения (АУПТ), системах противодымной защиты, а также в других автоматических системах безопасности и жизнеобеспечения, которые должны сохранять работоспособность в условиях пожара. Могут использоваться в сетях, работающих по таким стандартам, как RS-485, Profibus, CAN, LON и прочим. Могут использоваться на атомных станциях, в системах класса безопасности 2-4, вне гермозоны. Эксплуатируются внутри и вне помещений, при условии защиты от прямого воздействия солнечного излучения и атмосферных осадков. Допускается применение во взрывоопасных зонах любого класса по ГОСТ Р 51330.13.

Кабель КИС-РПнг(А)-FRHF 2х2х0,80 полностью удовлетворяет требованиям нормативных документов «Технического регламента о пожарной безопасности» ГОСТ 31565-2012, СП 5.13130.2009, СП 6.13130.2009.

Электрические свойства витой пары, как и любой другой направляющей системы электромагнитных колебаний, полностью характеризуются ее первичными параметрами: сопротивлением *R* и индуктивностью *L* проводников, а также емкостью *C* и проводимостью *G* изоляции.

Эти параметры (*R* и *G)* обусловливают потери энергии: первый – тепловые потери в проводе и экране (при его наличии), второй – потери в изоляции. Параметры *L* и *C* определяют реактивность витой пары как направляющей системы и, следовательно, её частотные свойства.

Конкретные значения первичных параметров зависят от конструкции кабеля и, в частности, от геометрии отдельных его компонентов, их взаимного расположения, материала проводников, изоляции и внешних покровов.

Исходные данные для расчетов: коэффициент скрутки 1,07; тангенс угла диэлектрических потерь изоляции из полиэтилена на частоте 550 кГц – $14 \cdot 10^{-4}$; эквивалентное значение относительной диэлектрической

проницаемости 2,0; толщина изоляции 0,4 мм; значение функции ψ = 0,75

a – расстояние между центрами жил для парной скрутки $a = \sqrt{2} d_1 = 1,06$ мм.

Расчет первичных параметров симметричного кабеля.

Активное сопротивление:

$$R_0 = \frac{4 \cdot 10^3 \cdot p\chi}{\pi d_0^2} \qquad (5.1)$$

$$R = \frac{2 \cdot 4 \cdot 10^3 \cdot 0,1754 \cdot 1,07}{\pi \cdot 0,75^2} = 80 \ \ Ом / км$$

Индуктивность:

$$L = \chi \left[4 \cdot \ln \frac{a - r_0}{r_0} + \mu \cdot Q\left(kr_0\right) \right] \cdot 10^{-4} \qquad (5.2)$$

$$L = 1,07 \left[4 \cdot \ln \frac{1,06 - 0,38}{0,38} + 0,7 \right] \cdot 10^{-4} = 1,07 \cdot 3 \cdot 10^{-4} = 0,35 \quad мГн / км.$$

Емкость:

$$C = \frac{\chi \varepsilon_Э \cdot 10^{-6}}{36 \cdot \ln\left(\frac{a}{r_0} \psi \right)} \qquad (5.3)$$

$$C = \frac{1,07 \cdot 2 \cdot 10^{-6}}{36 \cdot \ln\left(\frac{1,08}{0,38} \cdot 0,7 \right)} = \frac{2,4 \cdot 10^{-6}}{22,3} = 96,4 \qquad нФ / км$$

Проводимость:

$$G = \omega Ctg \, \delta_Э \qquad (5.4)$$

$$G = 6,3 \cdot 550 \cdot 10^3 \cdot 95,8 \cdot 10^{-9} \cdot 14 \cdot 10^{-4} = 465503 \cdot 10^{-10} \approx 482,23 \ \ мкСм / км$$

Расчет вторичных параметров симметричного кабеля.

Коэффициент затухания:

$$\alpha = 8,69\sqrt{\frac{\omega CR}{2}}, \qquad (5.5)$$

$$\alpha = 8,7\sqrt{\frac{6,3\cdot 550\cdot 10^{3}\cdot 95,8\cdot 10^{-9}\cdot 80}{2}} = 31,8 \ \ дБ/км$$

коэффициент фазы:

$$\beta = \sqrt{\frac{\omega CR}{2}} \qquad (5.6)$$

$$\beta = \sqrt{\frac{6,3\cdot 550\cdot 10^{3}\cdot 95,8\cdot 10^{-9}\cdot 80}{2}} = 4,1 \ рад/км$$

По результатам расчетов можно сделать вывод, что рассчитанные параметры симметричной сигнальной линии связи («витой пары») КИС-РПнг(А)-FRHF 2х2х0,80 комплексной системы безопасности офисного здания, удовлетворяют всем требованиям для бесперебойной передачи служебной информации.

ЗАКЛЮЧЕНИЕ

В настоящей выпускной квалификационной работе рассматривались актуальные вопросы обеспечения комплексной безопасности офисного здания. В процессе выполнения работы решены поставленные задачи:

– Изучены основы обеспечения комплексной безопасности офисного объекта, в том числе цели и задачи обеспечения безопасности, классификация угроз безопасности объекта, модель угроз и модель нарушителя, основные каналы проникновения на охраняемый объект, а также способы обнаружения нарушителя при проникновении на охраняемый объект.

– Разработаны схемы подсистем охранно-тревожной сигнализации, контроля и управления доступом и охранной телевизионной комплексной системы безопасности объекта электроэнергетики и выработаны соответствующие технические решения. Выбран состав

оборудования, удовлетворяющего техническому заданию на проектирование.

– Произведен расчет параметров комплексной системы безопасности, в том числе расчет резервного электропитания подсистем охранно-тревожной сигнализации, контроля и управления доступом и охранной телевизионной, а также расчет первичных и вторичных параметров симметричной сигнальной линии связи («витой пары») на базе кабеля КИС-РПнг(А)-FRHF 2х2х0,80 для бесперебойной передачи служебной информации в разработанной комплексной системы безопасности.

Считаю, что полученные в работе результаты можно использовать в практической деятельности подразделений вневедомственной охраны и ФГУП «Охрана» Росгвардии при обеспечении безопасности и антитеррористической защищенности офисных зданий.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации от 12 декабря 1993 г. (принята всенародным голосованием 12 декабря 1993 г.) [Электронный ресурс]. – Режим доступа: http://www.garant.ru/doc/constitution/.

2. Вопросы Федеральной службы войск национальной гвардии Российской Федерации: указ Президента Российской Федерации от 5 апреля 2016 г. № 157 [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/420346527.

3. О войсках национальной гвардии: федеральный закон от 3 июля 2016 года № 226-ФЗ.

4. Об антитеррористической защищенности объектов (территорий) (вместе с «Правилами разработки требований к антитеррористической защищенности объектов (территорий) и паспорта безопасности объектов (территорий): постановление Правительства Российской Федерации от 25 декабря 2013 № 1244 [Электронный ресурс]. – Режим доступа: http://base.garant.ru/70552494/.

5. Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 11 февраля 2017 г. № 176 [Электронный ресурс]. – Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71511840/.

6. О противодействии терроризму: федеральный закон от 6 марта 2006 г. № 35-ФЗ [Электронный ресурс]. – СПС «Консультант плюс». – URL : http // www.base.consultant. ru.

7. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 31 декабря 2015 г. № 683 [Электронный ресурс]. – СПС «Консультант плюс». – URL : http // www.base.consultant. ru.

8. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. – Введ. 2016-01-01. – Москва : Стандартинформ, 2014. – 27 с.

9. СП 132.13330.2011. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования.

10. СП 3.13130.2009. Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности.

11. СП 5.13130.2009. Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования.

12. Правила устройства электроустановок (Утверждены Приказом Минэнерго России от 08 июля 2002 г. № 204). – М.: Энергоатомиздат, Изд. 7., 2002. – 222 с.

13. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования. Введ. 2010-09-01. – Москва : Стандартинформ, 2010. – 32 с.

14. Ворона В.А. Комплексные интегрированные системы обеспечения безопасности [Электронный ресурс]: учебное пособие / Ворона

В. А., Тихонов В. А. – Электрон. Текстовые данные. – Москва: Горячая линия-Телеком, 2013. – 160 с. – Режим доступа: http://www.iprbookshop.ru/11989/ - ЭБС «IPRbooks», по паролю.

15. Ворона В.А. Технические системы охранной и пожарной сигнализации [Электронный ресурс]: учебное пособие / Ворона В. А., Тихонов В. А. – Электрон. Текстовые данные. – Москва: Горячая линия-Телеком, 2016. – 376 с. – Режим доступа: http://www.iprbookshop.ru/12052. - ЭБС «IPRbooks», по паролю.

16. Гречаный С.А. Проектирование технических систем безопасности и охранного мониторинга [Текст]: практикум / С.А. Гречаный [и др]. – Воронеж: Воронежский институт МВД России, 2018. – 125 с.

17. Р 78.36.002–2010. Выбор и применение систем охранных телевизионных : методические рекомендации. – М. : НИЦ «Охрана» МВД России, 2010. – 183 с.

18. Сидоров А.В. Процедура выбора оптимальной системы охраны при обеспечении охраны объекта // Охрана, безопасность, связь. – 2017 – №1-1. – С. 164-167

19. Винокуров С.А. Организация интегрированных систем безопасности и охранного мониторинга : курс лекций. Ч.1 / С.А. Винокуров, С.А. Гречаный, М.Ю. Пакляченко. – Воронеж: Воронежский институт МВД России, 2019. – 165 с.

20. Винокуров С.А. Организация интегрированных систем безопасности и охранного мониторинга : курс лекций. Ч.2 / С.А. Винокуров, С.А. Гречаный, М.Ю. Пакляченко. – Воронеж: Воронежский институт МВД России, 2019. – 158 с.