Федеральная служба войск национальной гвардии Российской Федерации

ГЛАВНОЕ УПРАВЛЕНИЕ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ
(ГУВО Росгвардии)

УТВЕРЖДЕНЫ
Начальником
ГУВО Росгвардии
генерал-лейтенант полиции
А. В. Грищенко
1 марта 2022 г.

РЕКОМЕНДАЦИИ

ПО ОХРАНЕ ОСОБО ВАЖНЫХ ОБЪЕКТОВ С ПРИМЕНЕНИЕМ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ

Р 089 – 2022

Москва 2022

АННОТАЦИЯ

В Рекомендациях приведены общие требования к интегрированным системам безопасности (ИСБ), требования к базовым системам ИСБ, общие требования к техническим средствам ИСБ, требования к отдельным вспомогательным и дополнительным системам ИСБ. Рассмотрены вопросы выбора, проектирования и ввода в эксплуатацию ИСБ. Приведена информация о применении ИСБ на взрывоопасных объектах. Представлены перспективы развития ИСБ, переход к PSIM (ПСИМ) – системам.

Рекомендации предназначены для инженерно-технических работников подразделений вневедомственной охраны войск национальной гвардии Российской Федерации, ФГУП «Охрана» Росгвардии и специалистов служб безопасности различных организаций, занимающихся вопросами выбора, проектирования и ввода в эксплуатацию ИСБ на объектах, в том числе взрывоопасных.

Содержание

Обозначения и сокращения

АРМ – автоматизированное рабочее место

АТС – автоматическая телефонная станция

БИ – блок излучателя

БП – блок приемника

ГОСТ – межгосударственный стандарт

ГОСТ Р – государственный стандарт Российской Федерации

ГУВО Росгвардии – Главное управление вневедомственной охраны Федеральной службы войск национальной гвардии Российской Федерации

ИСБ – интегрированная система безопасности

ИЭПВР – источник электропитания вторичный с резервом

КПП – контрольно пропускной пункт

КУД – контроль и управление доступом

МПХИГ – место проживания и хранения имущества граждан

ПО – программное обеспечение

ПУЭ – Правила устройства электроустановок

ПЦО – пункт централизованной охраны

РЭ – руководство по эксплуатации

СКУД – система контроля и управления доступом

СОС – система охранной сигнализации

СОТ – система охранная телевизионная

СПИ – система передачи извещений

СТН – система телевизионного наблюдения

СТС – система тревожной сигнализации

СУ – средства управления

СЦН – система централизованного наблюдения

ТС – техническое средство

ТУ – технические условия

УИ – исполнительное устройство

УПУ – устройство преграждающее управляемое

УС – устройство считывающее

ФГУП «Охрана» Росгвардии – Федеральное государственное унитарное предприятие «Охрана» Федеральной службы войск национальной гвардии Российской Федерации

ФКУ «НИЦ «Охрана» Росгвардии – Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации

ШС – шлейф сигнализации

ЭВМ – электронно-вычислительная машина

Термины и определения

В данных рекомендациях применены следующие термины с соответствующими им определениями.

автоматизированное рабочее место; АРМ – Персональное рабочее место, обеспечивающее автоматизацию взаимодействия сотрудника пункта централизованной охраны (мониторингового центра) с СЦН

антитеррористическая защита объекта – Деятельность, осуществляемая с целью повышения устойчивости объекта к террористическим угрозам

безопасность – Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз

взятие объекта под охрану – Штатное выполнение процедур по постановке объекта на охрану

видеокамера – Устройство, предназначенное для телевизионного анализа передаваемой сцены с помощью оптоэлектронного преобразования и передачи телевизионного сигнала

видеонаблюдение – Четкое изображение в пределах установленных зон при заданных уровнях освещенности и ожидаемых производственных помехах

вневедомственная охрана – Структурное подразделение Росгвардии, предоставляющее услуги по охране объектов всех форм собственности, а также МПХИГ

заказчик – Юридическое или физическое лицо, несущее ответственность за обеспечение противокриминальной защиты объекта

защищенность объекта – Уровень организационно-практических мероприятий, оснащения инженерно-техническими средствами охраны и действий персонала, направленных на предотвращение противоправных посягательств на объект, устранение или снижение угрозы здоровью и жизни людей от террористических актов и иных противоправных посягательств

зона охраны – Часть охраняемого объекта, оборудованная техническими средствами охраны и для которой установлен отдельный режим охраны

извещение – Передаваемая информация о состоянии охраняемого объекта или технического средства охраны

интерфейс – Совокупность средств и правил, обеспечивающая взаимодействие и сопряжение технических средств и модулей в составе системы централизованного наблюдения

исполнительное устройство; УИ – Устройство или механизм, обеспечивающее приведение УПУ в открытое или закрытое состояние

контроль и управление доступом; КУД – Комплекс организационно-технических мероприятий, направленный на предотвращение несанкционированного прохода людей или перемещение имущества

криминальная безопасность – Состояние защищенности личности, имущества, общества и государства от криминальных угроз

криминальная угроза – Совокупность условий и факторов, связанная с несанкционированным проникновением на охраняемый объект и/или совершением на его территории противоправных действий, в том числе террористических

локальная охрана – Охрана зон с передачей информации о состоянии технических средств охраны в пределах объекта

место проживания и хранения имущества граждан; МПХИГ – отдельные квартиры, индивидуальные жилые дома, коттеджи, дачи, гаражи, иные постройки, оборудованные техническими средствами охраны с подключением к пультам централизованного наблюдения подразделений вневедомственной охраны, а также камеры хранения имущества граждан, в том числе сейфовые и депозитные ячейки в хранилище

надежность технического средства (системы) охраны (безопасности) – свойство технического средства (системы) охраны (безопасности) сохранять во времени способность выполнять требуемые функции в

заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования

несанкционированный доступ – Доступ субъектов или объектов, не имеющих права доступа

нештатная ситуация – Положение нарушения охраны объекта, не предусмотренное регламентирующими документами

оповещатель звуковой – Оповещатель, выдающий звуковые неречевые сигналы

оповещатель световой – Оповещатель, выдающий световые сигналы

оповещатель – Техническое средство охранной, пожарной или охранно-пожарной сигнализации, предназначенное для оповещения людей на удалении от охраняемого объекта о проникновении или попытке проникновения и/или пожаре

особо важный объект – Техногенный, природный, природно-техногенный объект, подверженный риску криминальных угроз нанесения неприемлемого ущерба самому объекту, природе и обществу, а также подверженный угрозам возникновения чрезвычайных обстоятельств

охранный извещатель – Техническое средство охранной сигнализации, предназначенное для формирования тревожного извещения автоматическим или ручным способом при обнаружении проникновения (попытки проникновения) или других противоправных воздействий на охраняемый объект

охраняемый объект – Отдельное помещение или несколько помещений в одном здании, объединенные единым периметром, здания, строения, сооружения, прилегающие к ним территории и акватории, помещения, транспортные средства, а также грузы, денежные средства и иное имущество, подлежащее защите от противоправных посягательств

повышение надежности охраны – Комплекс организационно-технических мер, направленных на снижение риска нанесения ущерба от криминальных и террористических угроз

устройство преграждающее управляемое; УПУ – Устройство, обеспечивающее физическое препятствие доступу и оборудованное исполнительными устройствами для управления его состоянием (турникеты, шлюзы, проходные кабины, двери и ворота, оборудованные исполнительными устройствами СКУД, а также другие подобные устройства)

противокриминальная защита – Комплекс организационно-технических мер, осуществляемых с целью обеспечения криминальной безопасности объектов

пункт централизованной охраны (мониторинговый центр); ПЦО – Структурное подразделение организации, обеспечивающей круглосуточную централизованную охрану объектов с применением систем централизованного наблюдения в целях организации оперативного реагирования при поступлении информации о проникновении (попытке проникновения), а также о возникновении криминальных и технологических угроз

система контроля и управления доступом; СКУД – Совокупность совместно действующих технических средств, предназначенных для контроля и управления доступом и обладающих технической, информационной, программной и эксплуатационной совместимостью

система охранная телевизионная; СОТ – Телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной и антитеррористической защиты

система охранной сигнализации; СОС – Совокупность совместно действующих технических средств охраны (безопасности), предназначенных для обнаружения криминальных угроз, сбора, обработки, передачи и представления в заданном виде информации о состоянии охраняемого объекта или имущества

система передачи извещений; СПИ – Совокупность совместно действующих технических средств охраны, предназначенных для передачи по каналам связи и приема в ПЦО извещений о состоянии охраняемых объектов, служебных и контрольно-диагностических извещений, а также (при наличии обратного канала) для передачи и приема команд телеуправления

система телевизионного наблюдения; СТН – Совокупность функционирующих видеоканалов, программных и технических средств записи и хранения видеоданных, а также программных и/или технических средств управления, осуществляющих информационный обмен между собой

система тревожной сигнализации; СТС – Электрическая установка, предназначенная для обнаружения и сигнализации о наличии опасности

система централизованного наблюдения; СЦН – Совокупность программно-аппаратных средств и модулей, взаимодействующих в едином информационном поле, предназначенная для обнаружения криминальных и иных угроз на охраняемых объектах, передачи данной информации на ПЦО (мониторинговый центр), приема информации подсистемой пультовой и представления в заданном виде на ПЦН

снятие объекта с охраны – Штатное выполнение процедур по прекращению обеспечения техническими средствами охраны объекта

средства контроля и управления доступом; средства КУД – Механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом

средства управления; СУ – Аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со считывателей, проведение

идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации

техническое средство СОТ, ТС СОТ – Конструктивно и функционально законченное устройство, входящее в состав системы

централизованная охрана – Охрана территориально рассредоточенных объектов с помощью пунктов централизованной охраны

шлейф сигнализации; ШС – Электрическая цепь, линия связи, предназначенные для передачи извещений на средство сбора и обработки информации

штатная ситуация – Положение, при котором процесс обеспечения охраны объекта проходит в рамках процедур, предусмотренных регламентирующими документами

Введение

В настоящее время, в целях повышения надежности обеспечения противокриминальной и антитеррористической защищенности объектов, охраняемых подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации, активно применяются интегрированные системы безопасности. Это связано с повышением требований к уровню безопасности объектов различной ведомственной принадлежности, а также появлением на отечественном рынке новых средств автоматизации и информационных технологий, позволяющих интегрировать организационные и технические ресурсы для решения задач обеспечения, как имущественной, так и личной безопасности.

Использование ИСБ позволяет подразделениям вневедомственной охраны решить на новом качественном уровне задачи по обеспечению безопасности граждан и охраны собственности, повысить эффективность действий службы охраны и, тем самым, потенциально может предотвратить или свести ущерб к минимуму в тех случаях, когда он неизбежен.

Следует отметить, что применение ИСБ не устраняет необходимость контроля со стороны человека, но значительно повышает эффективность работы службы охраны, особенно при наличии многочисленных охраняемых зон и факторов риска. Оптимальное соотношение людских и технических ресурсов выбирается в соответствии с поставленными задачами и прогнозируемым уровнем угроз.

Вместе с тем, развитие и внедрение ИСБ осложнялось тем, что долгое время отсутствовал единый, согласованный со всеми заинтересованными ведомствами и организациями, разрабатывающими, выпускающими и применяющими ИСБ понятийный аппарат в данной области.

Для решения этой проблемы специалистами ФКУ «НИЦ «Охрана» Росгвардии совместно с ГУВО Росгвардии, в рамках деятельности технического комитета по стандартизации «Системы тревожной сигнализации и противокриминальной защиты» (ТК 234), был разработан национальный стандарт Российской Федерации ГОСТ Р 57674–2017, в котором устанавливаются основные положения функционального назначения ИСБ, их состава, а также вводится система терминов и их определений, предназначенных для формирования единого технического языка в области ИСБ с перспективой применения при разработке нормативных правовых актов Российской Федерации, ведомственных нормативно-технических документов, стандартов организаций, технических условий на ИСБ различных производителей и другой технической документации.

Приказом Федерального агентства по техническому регулированию и метрологии (Росстандарт) от 19 сентября 2017 года № 1142-ст данный национальный стандарт был утвержден и введен в действие с 1 июня 2018 года.

Стандарт распространяется на вновь разрабатываемые и модернизируемые ИСБ, предназначенные для обеспечения противокриминальной защиты объектов различных категорий, независимо от их формы собственности и ведомственной принадлежности.

В настоящих рекомендациях определены минимально необходимые тактико-технические параметры аппаратных средств и ПО ИСБ, предназначенных для охраны объектов, требования к системам, входящим в состав интегрированной системы, технические и организационные меры по защите информации в системах, даны предложения по выбору, проектированию, монтажу и вводу в эксплуатацию указанных систем.

При выборе, проектировании и монтаже ИСБ для защиты конкретного объекта, наряду с рекомендациями приведенными в данном издании, необходимо руководствоваться нормативными документами,

рекомендациями и методическими пособиями, список которых приведен в Приложениях А и Б, а также эксплуатационной документацией предприятий-изготовителей ТС ИСБ.

В соответствии со «Списком технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» для применения в подразделениях вневедомственной охраны рекомендованы следующие ИСБ: «Кодос А-20» (ОАО «КОДОС», г. Москва), «Ладога-А» (ООО НПП «Риэлта», г. Санкт-Петербург), «Р-08» (ООО «Викинг», г. Москва), «Стрелец-Интеграл» (ЗАО «Аргус-Спектр», г. Санкт-Петербург), «Орион» (ЗАО НВП «Болид», г. Королев, МО), «Рубеж-СБ» (ООО «КБ Пожарной Автоматики», г. Саратов). По всем перечисленным ИСБ проведены необходимые организационно-технические мероприятия:

- получены необходимые сертификаты;

- проведены технические экспертизы ИСБ;

- согласованы технические условия, в которых заданы параметры, соответствующие требованиям национальных и межгосударственных стандартов;

- проведены необходимые испытания, в том числе эксплуатационные, в подразделениях вневедомственной охраны.

Кроме того, со стороны ГУВО Росгвардии и ФКУ «НИЦ «Охрана» Росгвардии осуществляется постоянный контроль качества серийного производства ИСБ и авторский надзор за вносимыми в них схемными, конструктивными и программными изменениями.

ИСБ обеспечивают модульную структуру, позволяющую оптимально оборудовать охраняемые объекты любой сложности – от малых (отдельные торговые точки, гаражи и т.п.) до больших (крупные

промышленные предприятия, объекты социально-культурного назначения с массовым пребыванием людей и т.п.) инженерно-техническими средствами противокриминальной защиты.

Целью настоящих рекомендаций является оказание информационно-методической помощи подразделениям вневедомственной охраны, ФГУП «Охрана» Росгвардии, сотрудникам служб безопасности различных организаций при применении ИСБ, а также специалистам проектно-монтажных организаций при проектировании и оборудовании объектов ИСБ.

1 Общие требования к ИСБ

1.1 Требования к функциональному составу ИСБ и извещениям

В соответствии с терминологией, принятой ГОСТ Р 57674–2017, ***Интегрированная система безопасности – это система безопасности объекта, объединяющая в себе целевые функциональные системы, предназначенные для защиты от угроз различной природы возникновения и характера проявления.***

В стандарте определено, что в состав ИСБ должно входить не менее трех из следующих базовых систем:

- СТС;
- СОС;
- СОТ;
- СКУД.

Функциональная схема ИСБ, состоящей из базовых систем, приведена на рисунке 1.1.

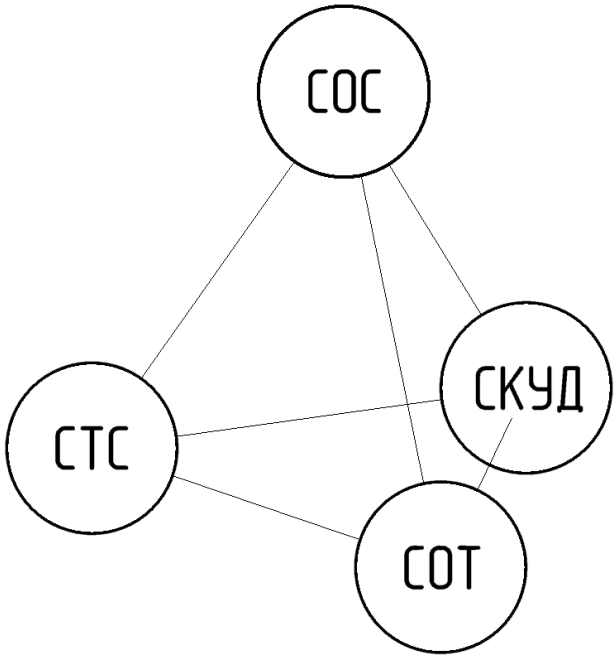


Рисунок 1.1

Допускается функциональное объединение СТС и СОС, при этом, в составе ИСБ их учитывают по отдельности.

ИСБ должна обеспечивать выполнение следующих обязательных функций:

- обнаружение угроз, имеющих различные причины возникновения и характер проявления, в соответствии с функциональным назначением систем, входящих в состав ИСБ;

- автоматическое реагирование ИСБ на обнаруженную угрозу, в соответствии с заданной тактикой работы каждой из систем, входящих в ее состав;

- передача информации о характере обнаруженной угрозы на устройства отображения, предназначенные для использования дежурным оператором;

- обеспечение возможности ручного управления системами, входящими в состав ИСБ;

- ведение электронного протокола функционирования систем, входящих в состав ИСБ, с регистрацией его в базе данных;

- модификация состава и конфигурации ИСБ, в соответствии с изменением задач, решаемых ИСБ.

Помимо обязательных, ИСБ может выполнять вспомогательные и дополнительные функции, не связанные с обеспечением противокриминальной безопасности. Состав ИСБ может быть дополнен иными системами обеспечения безопасности по ГОСТ Р 53195.1–2008.

При этом в состав ИСБ могут входить не все, а только необходимые вспомогательные и дополнительные системы. Пример функциональной схемы ИСБ, представляющей собой совокупность базовых, вспомогательных и дополнительных систем приведен на рисунке 1.2.

Рисунок 1.2

Предполагается, что системы, входящее в состав ИСБ должны обеспечить выполнение своих функций как в составе ИСБ, так и автономно, при этом состояние и режимы работы каждой из систем не должны создавать помехи в работе остальных систем и отказ (неисправность) одной из систем, не должен влиять на работоспособность прочих.

Наивысший приоритет передачи тревожных извещений и отображения информации в ИСБ отдается системам, направленным на обнаружение угрозы жизни и здоровью человека. Среди прочих, системы, предназначенные для обнаружения угрозы хищения, повреждения или уничтожения имущества имеют более высокий приоритет.

По виду организации противокриминальной защиты ИСБ подразделяются на локальные и централизованные.

Локальная ИСБ предназначена для обеспечения противокриминальной защиты отдельно взятого объекта, при которой

извещения о состоянии охраняемого объекта, а также управление осуществляют с помощью средств отображения информации и управления (индикаторные панели, пульты), входящих в состав ИСБ.

Централизованная ИСБ предназначена для обеспечения противокриминальной защиты объекта, охрана которого осуществляется при помощи системы централизованного наблюдения (СЦН).

В стандарте введены требования по составу обязательных извещений, передаваемых на автоматизированные рабочие места (АРМ) ИСБ (для локальных ИСБ) и АРМ СЦН (для централизованных ИСБ), а также отображаемых на внутренних и/или внешних устройствах отображения (оповещатели, индикаторы, индикаторные панели и т.п.).

К обязательным извещениям, передаваемым на АРМ, относятся следующие извещения:

- переход в дежурный режим;
- переход в тревожный режим;
- отключение основного электропитания и переход на резервное;
- восстановление основного электропитания;
- неисправность технических средств, входящих в состав ИСБ (в том числе – разряд аккумуляторных батарей), интерфейсов и линии связи;
- взятие объекта (зоны) под охрану;
- снятие объекта (зоны) с охраны.

К извещениям, отображаемым на внутренних и/или внешних устройствах отображения, относятся следующие извещения:

- переход в дежурный режим;
- переход в тревожный режим;
- взятие объекта (зоны) под охрану;
- снятие объекта (зоны) с охраны.

1.2 Принципы интеграции ИСБ

При объединении различных систем в составе ИСБ возможно применение нескольких типов интеграции.

Так, **аппаратную интеграцию** ИСБ осуществляют путем обеспечения аппаратной совместимости систем в составе ИСБ, посредством обмена информационными и управляющими сигналами, формируемыми при помощи коммутации электрических цепей.

Объединение систем производится на этапе проектирования системы для каждого конкретного объекта. Такая работа проводится проектно-монтажными организациями. Как правило, в этом случае, применяются разнородные системы различных производителей. Объединение (интеграция) этих систем осуществляется путем установки оборудования управления системами в общем помещении.

Очевидно, что это минимальный уровень интеграции, ему присущи известные недостатки («человеческий фактор», разнородность аппаратуры, сложность обслуживания, параллельность прокладываемых коммуникаций, отсутствие автоматизации и т.д.) и его нельзя считать в настоящее время перспективным.

Разновидностью такого типа интеграции, получившей наибольшее распространение, является интеграция посредством релейных выходов, используемых для передачи информационных сообщений между отдельными системами ИСБ.

Достоинствами данного типа интеграции является простота оборудования, невысокая стоимость, возможность объединения систем различных предприятий-изготовителей.

К недостаткам можно отнести:

- ограниченность видов извещений, которыми могут обмениваться системы;

- проблемы восприятия разнотипных способов представления информации о событиях и состоянии объединяемых систем;

- по мере роста количества реле и линий связи теряется преимущество низкой стоимости реализации. Суммарная стоимость релейной интеграции может превысить стоимость интеграции иного типа.

Программная интеграция (или более точно – интеграция на программно-аппаратном уровне с приоритетом программной поддержки). В этом случае роль объединения подсистем играет ПО, разработанное и поставляемое как самостоятельный продукт, предназначенный для функционирования в аппаратной среде, как правило, в локальной сети стандартных ЭВМ, которая представляет собой верхний уровень ИСБ. Сопряжение с аппаратной частью подсистем нижнего уровня осуществляется с помощью программ-драйверов, разрабатываемых специально для поддержки конкретных технических средств других предприятий-изготовителей. Связь с аппаратными средствами осуществляется с помощью стандартных портов ЭВМ.

Структурная схема ИСБ при программной интеграции приведена на рисунке 1.3.

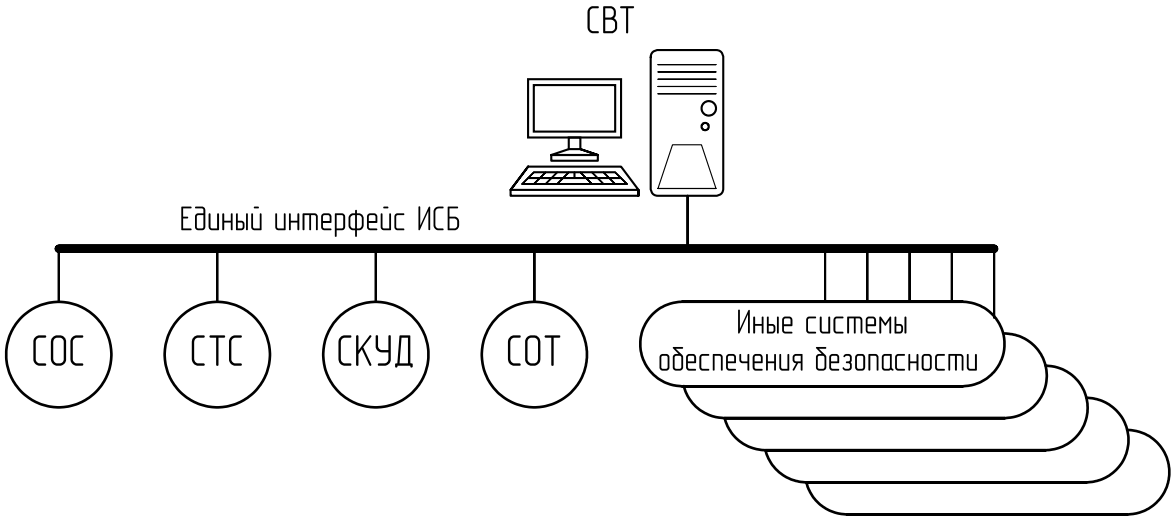


Рисунок 1.3

Существуют два подхода к созданию специализированного ПО для ИСБ:

- ПО разрабатывается под собственное оборудование и не позволяет работать с техническими средствами иных предприятий-изготовителей – «закрытое» ПО;

- ПО разрабатывается как «открытая» программная оболочка («открытое» ПО), с возможностью подключения оборудования различных предприятий-изготовителей.

Данная интеграция ИСБ имеет ряд положительных сторон. Это возможность на программном уровне, используя все преимущества современных компьютерных технологий, создавать высококачественные многофункциональные программные системы. Возможность интеграции с аппаратными средствами других предприятий-изготовителей (при наличии соответствующего драйвера и соответствующих интерфейсов обмена данными в самих применяемых средствах). Программная интеграция ИСБ требует меньшего количества линий связи между объединяемыми системами, по сравнению с аппаратной интеграцией.

С другой стороны, она не лишена недостатков – необходимость разработки драйверов для каждого применяемого аппаратного средства. При этом, разработчик аппаратного средства, не всегда предоставляет протоколы обмена данными. Даже, если протоколы «открыты» и документированы, в них могут быть заложены ограниченные возможности, не позволяющие оптимальным образом обеспечить сопряжение. Кроме того, разработчик ПО, поставляя только свой продукт, не может в этом случае в полном объеме гарантировать работу всей системы в целом.

Аппаратно-программная интеграция - наиболее распространенный тип интеграции ИСБ. В этом случае аппаратные и программные средства разрабатываются в рамках единой системы. Это позволяет достигнуть оптимальных характеристик, так как вся разработка сосредоточена, как правило, у одного предприятия-изготовителя и система

как законченный продукт поставляется с полной гарантией. При этом, возможно также получить оптимальные экономические показатели.

Недостатком здесь является то, что каждое предприятие-изготовитель ИСБ разрабатывает свои оригинальные технические решения, как правило, не совместимые с ИСБ других производителей.

Аппаратно-программная интеграция может включать четыре уровня. Пример функциональной схемы четырехуровневой ИСБ при аппаратно-программной интеграции приведен на рисунке 1.4.

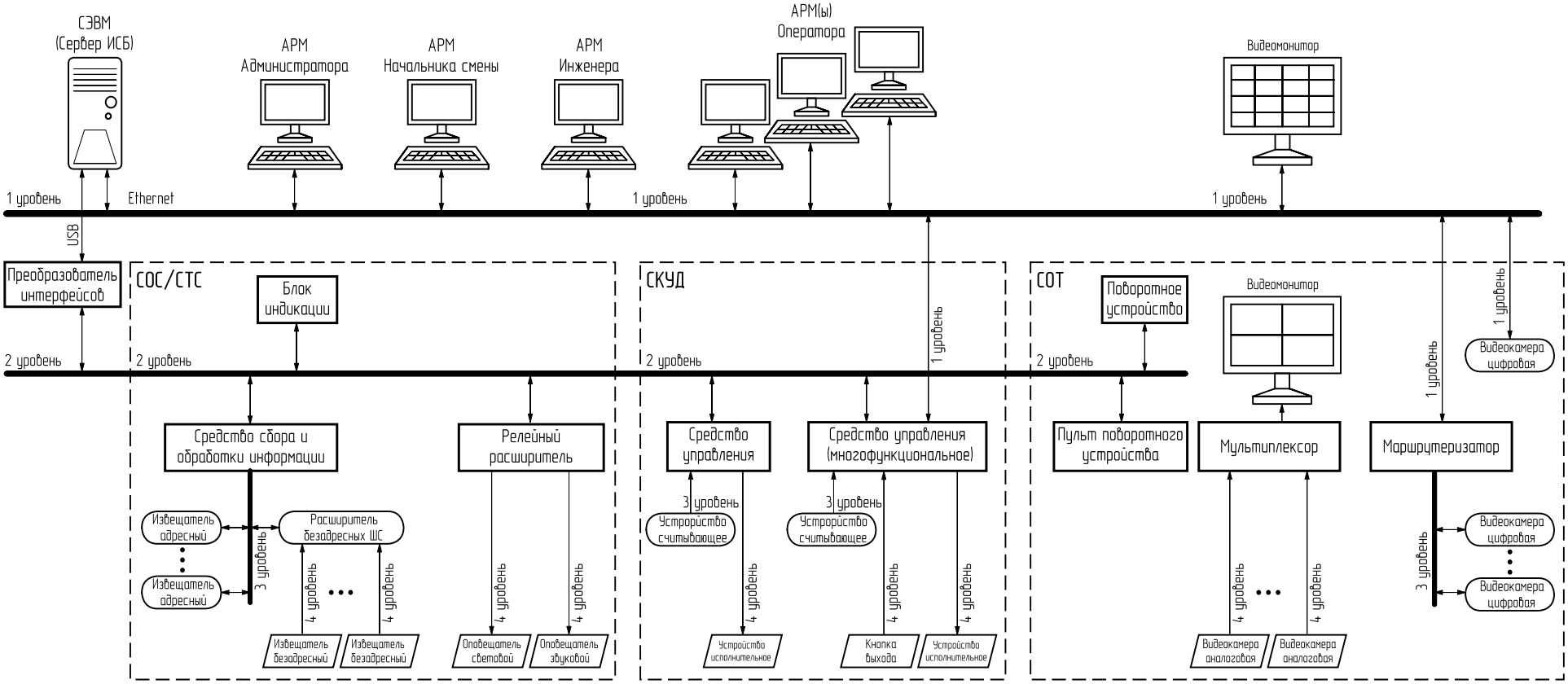

СЭВМ
(Сервер ИСБ)
АРМ
Администратора
АРМ
Начальника смены
АРМ
Инженера
АРМ(ы)
Оператора
Видеомонитор
1 уровень
Ethernet
1 уровень
1 уровень
USB
Преобразователь интерфейсов
2 уровень
СОС/СТС
Блок индикации
2 уровень
Средство сбора и обработки информации
Релейный расширитель
Извещатель адресный
Извещатель адресный
Расширитель безадресных ШС
3 уровень
4 уровень
4 уровень
Извещатель безадресный
Извещатель безадресный
4 уровень
4 уровень
Оповещатель световой
Оповещатель звуковой
СКУД
2 уровень
1 уровень
Средство управления
Средство управления (многофункциональное)
3 уровень
Устройство считывающее
3 уровень
Устройство считывающее
4 уровень
4 уровень
4 уровень
4 уровень
Устройство исполнительное
Кнопка выхода
Устройство исполнительное
СОТ
Поворотное устройство
2 уровень
Видеомонитор
1 уровень
Видеокамера цифровая
1 уровень
Пульт поворотного устройства
Мультиплексор
Маршрутизатор
4 уровень
4 уровень
3 уровень
Видеокамера цифровая
Видеокамера цифровая
Видеокамера аналоговая
Видеокамера аналоговая

Рисунок 1.4

Первый уровень аппаратно-программной интеграции ИСБ обеспечивает связь между сервером ИСБ, одним или несколькими АРМ, в том числе для территориально рассредоточенных объектов. Первый уровень аппаратно-программной интеграции ИСБ представляет собой локальную сеть на основе стандартов Ethernet и специализированного программного обеспечения.

Второй уровень аппаратно-программной интеграции ИСБ обеспечивает цифровой обмен данными между техническими средствами и представляет собой внутрисистемную сеть, реализованную на базе наиболее распространенных промышленных интерфейсов. Данная сеть должна взаимодействовать с сетью первого уровня посредством преобразования интерфейсов.

Третий уровень аппаратно-программной интеграции ИСБ представляет собой сеть или отдельные линии связи, обеспечивающие цифровой обмен данными между двумя функционально зависимыми техническими средствами.

Четвертый уровень аппаратно-программной интеграции ИСБ представляет собой электрические цепи и линии связи, предназначенные для обеспечения контроля и управления техническими средствами (ТС) без использования цифрового обмена данными (безадресные извещатели, оповещатели, релейные исполнительные устройства и др.).

2 Параметры базовых систем ИСБ

2.1 Общие положения

ИСБ должны соответствовать требованиям ГОСТ Р 57674–2017. Обязательным требованием является наличие общих ТУ, комплекта эксплуатационной документации, паспорт, руководство по работе с ПО и другие общесистемные документы). Помимо общей эксплуатационной документации, при необходимости, отдельные компоненты ИСБ могут комплектоваться частной эксплуатационной документацией. Поставка ИСБ заказчику должна производиться от одной вендорной компании, которая несет ответственность по гарантийным обязательствам по всем компонентам ИСБ.

АРМ локальных ИСБ должны исключать возможность автоматического (программного) сброса (пропадания с устройств визуального отображения информации) поступивших тревожных извещений, сброс (отработка) извещений должна осуществляться исключительно оператором АРМ.

Возникновение криминальной угрозы, выявленной СТС, СОС или СОТ должно переводить СКУД в режим реагирования на соответствующую криминальную угрозу, по алгоритму, учитывающему специфику защищаемого объекта.

Для обеспечения возможности сопряжения ИСБ с СПИ, получающими извещения о состоянии охраняемого объекта посредством замыкания/размыкания электрических контактов устройств объектовых оконечных, в составе ИСБ должны входить технические средства, имеющие релейные выходы, обеспечивающие тактику, согласующуюся с тактикой работы СПИ.

2.2 Параметры аппаратных средств и ПО ИСБ

Системы, входящие состав ИСБ, в зависимости от их функционального назначения, должны обеспечивать необходимый уровень надежности, пожарной безопасности, стойкости к воздействию внешних факторов.

Все компоненты ИСБ должны пройти процедуру подтверждения соответствия требованиям функционального назначения, безопасности, электромагнитной совместимости, и иметь подтверждающие документы.

Технические характеристики протоколов обмена информацией и интерфейсов ИСБ должны указываться в ТУ и эксплуатационной документации на конкретные компоненты.

Общие требования к ПО ИСБ, заданные в ТУ должны соответствовать ГОСТ 28195–89.

ПО ИСБ должно быть устойчиво к следующего вида:

- отключение электропитания;
- программный сброс;
- аппаратный сброс технических средств;
- случайное нажатие клавиш на клавиатуре;
- случайный перебор пунктов меню.

После указанных воздействий и перезапуска ПО, должна обеспечиваться работоспособность ИСБ и сохранность настроек и ранее полученных данных.

ИСБ должно обеспечивать возможность одновременного использования нескольких типов АРМ с разделением операторов АРМ по предоставленным полномочиям и правам доступа: просмотр информации, управление ИСБ, администрирование.

2.3 Технические и организационные мероприятия по защите информации ИСБ

В системах ИСБ должны быть приняты следующие меры по защите информации:

- защита компонентов ИСБ от несанкционированных действий внешних и внутренних нарушителей;
- защита информации в линиях связи и местах ее хранения.

Технические мероприятия по защите информации и обеспечению внутренней безопасности ИСБ необходимо строить по следующим направлениям:

- ограничение доступа к местам размещения пультов АРМ, пультов управления ИСБ;
- идентификация пользователей ИСБ;
- разграничение прав пользователей по доступу к информации;
- регистрация и учет работы пользователей;
- антивирусная защита ПО с возможностью восстановления информации, поврежденной вирусными воздействиями;
- резервирование важных для функционирования ИСБ областей данных;
- кодирование информации;
- контроль вскрытия аппаратуры.

Организационные мероприятия по защите информации заключаются в разработке и реализации административных и организационных мер по подготовке к эксплуатации ИСБ. К ним относятся:

- ограничение количества должностных лиц, допущенных к работе с ИСБ;
- размещение технических средств в отдельных режимных помещениях;

- разделение функций технического обслуживания и ремонта от функций администрирования ИСБ;

- периодическая смена паролей.

Перечисленные выше мероприятия дополняются следующими мерами:

- постановка на учет носителей информации и документации;

- проверка отсутствия посторонней аппаратуры;

- защита аппаратуры от электромагнитного излучения и наводок;

- периодическая проверка системы контроля вскрытия аппаратуры.

ПО ИСБ должно быть защищено от несанкционированного доступа.

Рекомендуемые уровни защиты доступа к ПО ИСБ с помощью паролей с разделением по типу пользователей:

- первый («**администратор**») – доступ ко всем функциям;

- второй («**дежурный оператор**») – доступ только к функциям текущего контроля;

- третий («**системный оператор**») – доступ к функциям конфигурации ПО без доступа к функциям управления СКУД.

Количество знаков в пароле должно быть не менее шести, при этом рекомендуется при составлении пароля использовать строчные и прописные буквы латинского алфавита, цифры, символы.

При вводе пароля в систему, вводимые знаки не должны отображаться на средствах отображения информации. Введенные пароли должны быть защищены от просмотра средствами операционных систем ЭВМ.

2.4 Параметры СОС и СТС

СОС и СТС, входящие в состав ИСБ, должны:

- осуществлять контроль состояния ШС;

- осуществлять контроль работоспособности и состояния входящих в нее ТС, интерфейсов и линии связи (в случае возможности технического осуществления такого контроля);

- осуществлять управление постановкой и снятием с охраны;

- обеспечивать возможность формирования и передачи тревожных и служебных извещений на АРМ локальной ИСБ и (или) АРМ СЦН;

- обеспечивать работоспособность при отключении основного источника электропитания, получая электропитание от резервного источника электропитания, в течение времени, необходимого для восстановления работоспособности основного источника электропитания (конкретное значение времени зависит от категории электроснабжения защищаемого объекта и должно указываться в технической документации на ИСБ);

- не выдавать ложных извещений при переходе электропитания с основного источника электропитания на резервный и обратно.

В СОС и СТС должна быть исключена возможность игнорирование состояния ШС программными методами.

Адресные и безадресные ШС СОС и СТС должны соответствовать требованиям ГОСТ 52436–2005.

Время от момента перехода любого адресного извещателя в тревожный режим до момента отображения тревожного извещения на световых и звуковых охранных оповещателях, индикаторных панелях, пультах управления, АРМ не должно превышать 10 с.

В СОС и СТС должны быть реализованы функции управления внешними световым и звуковым оповещателями со следующей тактикой оповещения.

Для светового оповещателя:

- СОС снят с охраны – оповещатель находится в режиме отсутствия свечения;

- СОС и СТС в дежурном режиме – оповещатель находится в режиме непрерывного свечения;

- СОС и СТС в тревожном режиме – оповещатель находится в режиме прерывистого свечения с частотой повторения от 0,5 до 2 Гц.

Для звукового оповещателя:

- СОС снят с охраны, СОС и СТС в дежурном режиме – оповещатель выключен;

- СОС и СТС в тревожном режиме – оповещатель включен на ограниченное время.

ТС, входящие в состав СОС и СТС, должны иметь возможность программного или аппаратного задания следующих тактик работы релейных выходов: «охранный ПЦН», «световой оповещатель», «звуковой оповещатель».

Требования к устройствам постановки/снятия с охраны

ТС СОС и СТС, производящие постановку/снятие с охраны при помощи клавиатуры должны применять коды разрядностью не менее четырех знаков. В СОС и СТС, использующих такие ТС должна быть предусмотрена защита от подбора кода (при троекратном введении неверного кода должно происходить временное блокирование возможности введения кода, а после троекратного блокирования – формироваться извещение о тревоге).

В ТС, с помощью которых осуществляется постановка на охрану и снятие с охраны, не допускается применение в качестве устройств снятия с охраны тумблеров, кнопок и т.п.

Изменение настроек и режимов работы ТС СОС и СТС должно быть невозможно при нахождении СОС и СТС в режиме охраны.

Сигналы СТС должны отличаться от других сигналов.

В качестве вызывных устройств СТС используются неавтоматические (с ручным, или ножным, управлением) охранные извещатели – электромеханические кнопки, радиокнопки, радиобрелоки,

педали, а также устройства подачи тревоги вне зависимости от действия персонала (устройства, оснащенные датчиками падения, наличия пульса, дыхания, а также устройства типа «ловушек»: оптикоэлектронные барьеры; устройства, выполненные в виде предметов, привлекающих внимание нападающих и оснащенных датчиками сигнализации; другие средства аналогичного назначения).

СТС должна работать по принципу «без права отключения», во время нахождения людей на охраняемом объекте.

Вызывные устройства СТС должны устанавливаться:

- в кабинетах руководителей;
- в помещениях службы охраны;
- на постах и в помещениях охраны, расположенных в здании, строении, сооружении и на охраняемой территории;
- в помещениях КПП, бюро пропусков;
- в помещениях критических элементов объекта;
- на маршрутах передвижения охраны;
- в других помещениях, в которые возможно проникновение нарушителей во время нахождения там персонала объекта;
- в хранилищах, кладовых, сейфовых комнатах;
- в помещениях хранения оружия и боеприпасов;
- на рабочих местах кассиров;
- у центрального входа в здание и запасных выходах из него;
- в коридорах, у дверей и проемов, через которые производится перемещение ценностей;
- на охраняемой территории у центрального входа (въезда) и запасных выходах (выездах);
- в других местах по требованию руководителя объекта или по рекомендации службы безопасности или охранной организации.

Извещатели СТС должны размещаться в местах, по возможности незаметных для посторонних.

Руководителей объекта, сотрудников службы безопасности и охраны следует оснащать мобильными беспроводными устройствами СТС (радиокнопками или радиобрелоками).

2.5 Параметры СКУД

СКУД должны соответствовать требованиям ГОСТ Р 51241–2008. ТС СКУД, относящиеся к УПУ, должны соответствовать требованиям ГОСТ Р 54831–2011.

СКУД должны обеспечивать:

- санкционированный доступ людей, транспорта и других объектов в (из) помещения, здания, зоны и территории, путем идентификации личности по комбинации различных признаков: вещественный код (ключи, карты, брелоки), запоминаемый код (клавиатуры, кодонаборные панели и другие аналогичные устройства), биометрический (отпечатки пальцев, сетчатка глаз и другие);

- предотвращение несанкционированного доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории;

- взаимодействие с другими системами ИСБ, с целью обеспечения противокриминальной защиты защищаемого объекта.

В состав СКУД должны входить:

- УС в составе считывателей и идентификаторов;

- СУ в составе аппаратных и программных средств;

- УПУ в составе преграждающих конструкций и исполнительных устройств.

СКУД должна выполнять следующие основные функции:

- открывание УПУ после считывания идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение или территорию) в заданный временной интервал или по команде оператора СКУД;

- запрет открывания УПУ после считывания идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение или территорию) в заданный временной интервал;

- санкционированное изменение (добавление, удаление) идентификационных признаков в СУ и связь их с зонами доступа (помещениями) и временными интервалами доступа;

- защиту от несанкционированного доступа к программным средствам СУ для изменения (добавления, удаления) идентификационных признаков;

- защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации в виде системы паролей и идентификации пользователей;

- сохранение настроек и базы данных идентификационных признаков при отключении электропитания;

- ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при чрезвычайных ситуациях, пожаре, при технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

- открытие или блокировку любых дверей, оборудованных СКУД, с рабочего места оператора системы;

- автоматическое открытие определенных дверей по пожарной тревоге,

- автоматическое закрытие УПУ при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;

- закрытие УПУ на определенное время и выдачу сигнала тревоги при попытках подбора идентификационных признаков (кода);

- отображение на пульте оператора, регистрацию и протоколирование текущих и тревожных событий;

- возможность просмотра и печати протокола работы системы (действия оператора, системные события, проходы клиентов, тревоги и аварийные ситуации);

- автономную работу считывателя с УПУ в каждой точке доступа при отказе связи с СУ;

- возможность архивирования базы и просмотра архива в автономном режиме;

- возможность распределения сотрудников по структуре предприятия для удобства работы с базой клиентов системы;

- возможность идентификации сотрудников и посетителей объекта по фотографиям из базы системы при проходе через турникеты (проезде через ворота);

- возможность отображения на пульте оператора графической схемы объекта с указанием местоположения дверей, турникетов и других конструкций с установленными на них считывателями;

- учет клиентов системы по типу пропусков:

- постоянные пропуска (действуют на все время работы сотрудника);

- временные пропуска (действуют на определенный срок и удаляются из системы автоматически по окончании этого срока);

- гостевые пропуска (дают право прохода на одно посещение).

УС должны обеспечивать:

- считывание идентификационного признака с идентификаторов;

- обмен информацией с СУ.

УС должно быть защищено от манипулирования путем перебора или подбора идентификационных признаков.

Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов.

СУ должно обеспечивать:

- прием информации от УС, ее обработку, отображение в заданном виде и выработку сигналов управления УПУ;

- введение баз данных работников объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и другие);

- ведение электронного журнала регистрации прохода работников через точки доступа;

- приоритетный вывод информации о тревожных ситуациях в точках доступа;

- контроль исправности состояния УПУ, УС и линий связи.

СКУД должна обеспечивать организацию пропускного и внутриобъектового режима на объектах и предусматривать разделение объекта на три основные зоны доступа:

- **первая зона** – здания, территории (локальные зоны), помещения, доступ в которые персоналу и посетителям не ограничен;

- **вторая зона** – помещения (локальные зоны), доступ в которые разрешен ограниченному составу персонала, а также посетителям объекта по разовым или временным пропускам или в сопровождении персонала объекта;

- **третья зона** – специальные помещения объекта, доступ в которые имеют строго определенные сотрудники и руководители.

Пропуск работников на объект через точки доступа должен осуществляться:

- в первой зоне доступа по одному признаку идентификации;

- во второй зоне доступа – по двум признакам идентификации (например, электронная карточка и ключ от механического замка);

- в третьей зоне доступа – не менее чем по двум признакам идентификации.

СКУД рекомендуется оборудовать:

- въездную группу (управление шлагбаумом на центральном въезде-выезде);

- турникеты входов в здание;

- кабинеты руководства;

- двери выходов из лифтовых холлов;

- служебные входы;

- помещения охраны;

- помещения, в которых непосредственно сосредоточены материальные ценности;

- режимные помещения и зоны ограниченного доступа (АТС, серверные, кроссовые, аппаратные, диспетчерские пункты, помещения жизнеобеспечения здания и т.п.);

помещения, согласованные с руководителем объекта дополнительно в ходе проектирования.

СКУД должна содержать следующие АРМ:

- АРМ администратора;

- АРМ дежурного оператора охраны;

- АРМ оператора на проходной;

- АРМ бюро пропусков;

- АРМ отдела кадров.

Функции отдельных АРМ СКУД могут объединяться на одном рабочем месте.

2.6 Параметры СОТ

СОТ должна соответствовать требованиям ГОСТ Р 51558–2014.

СОТ должна обеспечивать передачу визуальной информации о состоянии охраняемых зон, помещений, периметра и территории объекта на локальный АРМ СОТ. Применение СОТ позволяет в случае получения извещения о тревоге определить характер нарушения, место нарушения, направление движения нарушителя и определить оптимальные меры противодействия.

СОТ, предназначенная для работы в автоматизированном режиме, применяется в составе ИСБ или в дополнение к СОС. Видеоизображение в СОТ выводится на видеомонитор оператора только в случае возникновения тревоги (по сигналу тревоги, получаемому от извещателя охранной сигнализации, который логически связан с данной камерой видеонаблюдения). Задача СОТ в данном случае предоставить оператору дополнительную информацию о состоянии охраняемой зоны. Например, с целью исключения ложных тревог или с целью включения видеозаписи для последующего анализа ситуации или контроля действий службы охраны.

Видеокамеры СОТ могут также включаться по сигналу видеодетектора движения (аппаратного устройства или программно реализованного в составе АРМ СОТ), однако видеодетектор движения не может использоваться в качестве охранного извещателя СОТ.

СТН, как частный случай применения СОТ, предназначена для работы в неавтоматизированном режиме и используется для видеонаблюдения за обстановкой на контролируемом объекте (помещении, зоне) в реальном времени. Для работы СТН требуется организация отдельного поста видеонаблюдения и дежурного оператора видеонаблюдения.

СОТ должны обеспечивать возможность выполнения следующих функций:

- визуальный контроль объектов охраны и прилегающих к ним территорий;

- оперативный контроль действий персонала службы безопасности (подразделения охраны) и предоставление необходимой информации для координации этих действий;

- архивирование видеоинформации для последующего анализа событий;

- программирование режимов работы;

- функционирование под управлением систем контроля и управления доступом и охранной сигнализации.

Современные СОТ, строящиеся по цифровым технологиям (цифровые видеосистемы) на базе компьютерной техники и/или специализированных цифровых устройств обработки видеоинформации, имеют преимущества перед аналоговыми системами, позволяют организовать более эффективную систему охраны объектов.

Цифровые СОТ обеспечивают выполнение ряда дополнительных функций:

- предоставление наглядного отображения состояний и управление элементами СОТ на компьютерном мониторе с использованием графических планов объекта разных уровней детализации;

- разграничение полномочий операторов, администратора и инсталлятора системы с целью предотвращения неквалифицированного и/или несанкционированного управления;

- настройку нескольких зон контроля для каждой телекамеры, что позволяет обнаруживать движение в определенных частях кадра;

- цифровое (2/4/8/16-кратное) увеличение для детального анализа событий и идентификации лиц, предметов, номерных знаков автомобилей и т.п.;

- воспроизведение видеозаписи с использованием любого режима отображения на экране монитора;

- запись видеоинформации на внутренние носители по принципу ленты, замкнутой в кольцо;

- использование индивидуальной для каждой телекамеры настройки условий и продолжительности записи во время регистрации тревожных ситуаций;

- осуществление цифровой мультиплексной записи одновременно по всем телекамерам;

- программирование приоритета при записи первых мгновений тревожных событий (повышенная частота записи видеоинформации по тревожному каналу при сохранении обычного режима для остальных телекамер);

- программирование времени и скорости записи предтревожной ситуации и автоматическое отображение ее при появлении тревоги;

- программирование режимов записи в зависимости от приходящих внешних сигналов тревоги и наличия движений в кадре. Запись событий может включаться по сигналу тревоги на заданное время, сохранять одиночный кадр или вестись непрерывно;

- оперативный доступ к любому записанному кадру или последовательности кадров путем задания времени, даты и идентификатора телекамеры;

- распечатку любого экранного изображения на подключенном к системе принтере и/или экспорт его на сменный носитель для последующего изучения или распечатки на другом компьютере и др.

На объекте СОТ следует оборудовать:

- периметр территории;

- проходные, КПП автомобильного и железнодорожного транспорта;

- помещения постов охраны (на случай нападения на пост и в целях контроля несения службы);

- досмотровые помещения (комнаты), зоны досмотра транспорта; стоянки транспорта;

- главный и запасные входы/выходы;

- критические и уязвимые места и зоны объекта;

- помещения, коридоры, по которым производится перемещение денежных средств и материальных ценностей;

- помещения, в которых непосредственно сосредоточены материальные ценности, за исключением хранилищ ценностей;

- погрузочные терминалы;

- хранилища товарной продукции;

- хранилища вредных и опасных веществ;

- узлы управления технологическими процессами;

- другие помещения по усмотрению руководителя (собственника) объекта или по рекомендации службы безопасности.

Телекамеры, предназначенные для контроля территории объекта или ее периметра, должны работать при температуре окружающего воздуха от минус 40°С до плюс 50°С (от минус 50°С до плюс 55°С для климатических зон с холодным климатом) и размещаться в герметичных термокожухах, имеющих солнцезащитный козырек.

Телекамеры должны быть ориентированы на местности под углом к линии горизонта (лучи восходящего и заходящего солнца не должны попадать в объектив). Следует учитывать направление света фар транспорта, движущегося вблизи зоны просмотра во избежание «засветок» телекамеры.

Размещение телекамер должно препятствовать их умышленному повреждению или краже. При необходимости возможна установка дополнительной защиты телекамер и применение автоматических устройств контроля наличия видеосигнала.

В темное время суток, если освещенность охраняемой зоны ниже чувствительности телекамер, должно включаться охранное освещение видимого или инфракрасного диапазона света. Зоны охранного освещения должны совпадать с зоной обзора телекамер. Для цветных видеокамер, не имеющих черно-белого режима, допустимо применение подсветки только видимого диапазона.

Для детального наблюдения обстановки на больших территориях рекомендуется использовать телекамеры, оснащенные поворотными устройствами и трансфокаторами.

Для наблюдения с помощью одной телекамеры больших территорий объекта должны применяться объективы с переменным фокусным расстоянием и поворотные устройства с дистанционным управлением.

Предпочтительно использование моноблочных, в том числе, купольных роботизированных поворотных камер цветного изображения. Скорость позиционирования телекамеры в зону наблюдения не должна превышать единиц секунд.

В помещениях объекта рекомендуется использовать телекамеры с электронным затвором, укомплектованные объективом с ручной регулировкой диафрагмы (в случаях отсутствия резкого изменения освещенности). При установке телекамеры против мощного источника света (окно, лампа, и др.) следует применять телекамеры со встроенной автоматической компенсацией засветки.

Вне помещений объекта (на улице) рекомендуется комплектовать телекамеры объективом с автоматической регулировкой диафрагмы.

В СОТ следует использовать обнаружители движения (видеодетекторы), обеспечивающие выдачу сигнала тревоги на АРМ СОТ при появлении в поле зрения видеокамеры движущейся цели. При наличии в СОТ функции детектора движения, возможно создание дополнительного рубежа охраны. В этом случае тревожный сигнал от дополнительного рубежа охраны должен поступать на АРМ СОТ в виде звукового и визуального оповещения.

Видеодетекция движения позволяет привлечь внимание оператора к перемещениям в охраняемой зоне. Задаются различные зоны видеодетекции и параметры чувствительности (настройки на размер и контрастность объектов, продолжительность и направление движения и т.д.). При обнаружении движения в охраняемой зоне система выводит оператору изображение с камеры в зоне срабатывания, выделяет камеру на плане объекта и выдает звуковое сообщение.

Вся видеоинформация должна записываться на цифровые видеорегистраторы.

С целью сокращения объема видеоархива, допускается осуществлять видеозапись только по сигналам видеодетектора, или извещателей, зона обнаружения, которых связана с полем зрения видеокамеры, при наличии функции отката изображения.

В качестве устройств управления и коммутации видеосигналов, поступающих с телекамер, следует использовать последовательные переключатели, квадраторы, матричные коммутаторы. Они должны обеспечивать последовательное или полиэкранное воспроизведение изображений от всех телекамер.

Устройства управления и коммутации должны обеспечивать приоритетное автоматическое отображение на экране мониторов зон, откуда поступило извещение о тревоге.

Конструктивно СОТ должна строиться по модульному принципу и обеспечивать:

- взаимозаменяемость сменных однотипных технических средств;
- удобство технического обслуживания, ремонта и эксплуатации;
- исключение несанкционированного доступа к элементам управления;
- санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

3 Общие параметры тс ИСБ

3.1 Параметры надежности

Параметры надежности ТС ИСБ должны определяться по ГОСТ 27.003–2016 и соответствовать требованиям стандартов на технические средства конкретных видов и ТУ на ТС конкретных типов.

Гарантийный срок эксплуатации ТС ИСБ должен быть не менее 5 лет, за исключением элементов, подлежащих замене в процессе эксплуатации.

Срок службы ТС ИСБ должен составлять не менее 8 лет.

Средняя наработка до отказа невосстанавливаемых (неремонтируемых) ТС ИСБ должна быть не менее 60000 ч, средняя наработка на отказ восстанавливаемых (ремонтируемых) ТС ИСБ должна быть не менее 30000 ч.

Для ТС ИСБ, функционирование которых характеризуется числом коммутационных циклов, средняя наработка до отказа должна быть не менее 1 000 000 рабочих циклов в электрических режимах коммутации, установленных в стандартах на ТС конкретных видов или в ТУ на ТС конкретных типов.

3.2 Параметры электромагнитной совместимости

ТС ИСБ в зависимости от области применения и условий эксплуатации должны обеспечивать помехоустойчивость при воздействии электромагнитных помех следующих степеней жесткости по ГОСТ Р 50009–2000:

- вторая степень – для ТС ИСБ, предназначенных для эксплуатации в закрытых помещениях;

- третья степень – для ТС ИСБ, предназначенных для эксплуатации на открытых площадках и периметрах территорий.

Уровни индустриальных радиопомех, создаваемых ТС ИСБ, при функционировании, должны соответствовать нормам по ГОСТ Р 50009–2000, в зависимости от области применения и условий эксплуатации, установленных в ТУ на ТС конкретных типов.

3.3 Параметры безопасности

ТС ИСБ должны удовлетворять общим требованиям безопасности, установленным в ГОСТ Р 52435–2015, стандартах на ТС конкретных видов и ТУ на ТС конкретных типов.

Конструктивное исполнение ТС ИСБ должно обеспечивать их пожарную безопасность по ГОСТ IEC 60065–2013 в аварийном режиме работы и при нарушении правил эксплуатации.

Значения электрической прочности изоляции ТС ИСБ должны соответствовать требованиям ГОСТ Р 52931–2008, а также стандартов на ТС конкретных видов и ТУ на ТС конкретных типов.

Значения электрического сопротивления изоляции цепей ТС ИСБ должны соответствовать требованиям ГОСТ Р 52931–2008, а также стандартов на ТС конкретных видов, ТУ на ТС конкретных типов.

Конкретные значения сопротивления изоляции и электрическая прочность изоляции должны быть указаны в ТУ и эксплуатационных документах на ТС конкретных типов.

ТС ИСБ, предназначенные для эксплуатации в зонах с взрывоопасной средой, должны соответствовать требованиям ТР ТС 012/2011.

3.4 Параметры устойчивости к климатическим и механическим воздействиям

Требования устойчивости ТС ИСБ к воздействию климатических и механических факторов должны быть установлены в ТУ на ТС конкретных типов в соответствии с требованиями ГОСТ Р 54455–2011, а также определяться требованиями стандартов на ТС конкретных видов, исходя из области применения и условий эксплуатации ТС.

3.5 Параметры электропитания

Электропитание ТС ИСБ допускается осуществлять от:

- электрической сети систем электроснабжения общего назначения (электрическая сеть);
- ИЭПВР по ГОСТ Р 53560–2009;
- других ТС ИСБ, имеющих специально предназначенные для этого выходы;
- автономных источников электропитания.

Электропитание отдельных ТС ИСБ допускается осуществлять от других источников с иными параметрами выходных напряжений, требования к которым устанавливаются в нормативных документах на конкретные типы ТС.

ТС ИСБ, электропитание которых осуществляется от однофазной электрической сети переменного тока номинальным напряжением 230 В (по ГОСТ 29322–2014). ТС должны сохранять работоспособность при отклонении напряжения электропитания от номинального значения в пределах от минус 20 % до плюс 10 %.

ТС ИСБ, электропитание которых осуществляется от ИЭПВР, должны сохранять работоспособность при отклонении напряжения

электропитания от номинального значения напряжения (12 В или 24 В) на ± 15 %.

ТС ИСБ должны иметь резервное электропитание при пропадании напряжения основного источника электропитания. В качестве резервных источников электропитания может использоваться резервная сеть переменного тока или источники электропитания постоянного тока.

Переход с основного на резервное электропитание и обратно должен происходить автоматически без нарушения установленных режимов работы и функционального состояния ТС ИСБ.

Резервные источники электропитания должны обеспечивать выполнение основных функций ТС ИСБ при пропадании напряжений в сети на время, определяемое действующими нормативными документами для каждого ТС.

Допускается не применять резервирование электропитания с помощью аккумуляторных батарей для УПУ СКУД, которые требуют для управления значительных мощностей приводных механизмов (приводы ворот, шлюзы и т.п.). При этом, такие УПУ должны быть оборудованы аварийными механическими средствами открывания, и иметь системные средства индикации аварии электропитания.

При использовании в качестве источника резервного электропитания аккумуляторных батарей, должен выполняться их автоматический заряд.

В ТС ИСБ рекомендуется применять резервные источники электропитания позволяющие осуществлять удаленный контроль (на АРМ ИСБ) их состояние и основные параметры электропитания.

Автономные (химические) источники электропитания, встроенные в идентификаторы СКУД, беспроводные извещатели систем охранной и тревожной сигнализации, должны обеспечивать работоспособность в течение времени, не менее трех лет.

4 Параметры отдельных вспомогательных и дополнительных систем ИСБ

4.1 Параметры системы оповещения

Система оповещения на охраняемом объекте и его территории создается для оперативного информирования людей о тревоге или чрезвычайном происшествии (аварии, пожаре, стихийном бедствии, нападении, террористическом акте) и координации их действий.

На объекте должен быть разработан план оповещения, который в общем случае включает в себя:

- схему вызова сотрудников, должностными обязанностями которых предусмотрено участие в мероприятиях по предотвращению или устранению последствий внештатных ситуаций;
- инструкции, регламентирующие действия сотрудников при внештатных ситуациях;
- планы эвакуации;
- систему сигналов оповещения.

Система оповещения должна обеспечивать возможность выполнения следующих функций:

- подачу звуковых, и (или) световых, и (или) речевых сигналов в здания, помещения, на участки территории объекта с постоянным или временным пребыванием людей;
- подачу звуковых, и (или) световых, и (или) речевых сигналов операторам АРМ, дежурным службы безопасности объекта;
- приоритетную подачу сигналов операторам АРМ, дежурным службы безопасности объекта;
- трансляцию речевой информации о характере опасности, необходимости и путях эвакуации, других действиях, направленных на обеспечение безопасности людей.

Сигналы оповещения должны отличаться от сигналов другого назначения.

Количество оповещателей, их мощность должны обеспечивать слышимость во всех местах постоянного или временного пребывания людей.

На охраняемой территории следует применять рупорные громкоговорители. Они могут устанавливаться на опорах освещения, стенах зданий и других конструкциях.

Правильность расстановки и количество громкоговорителей на объекте определяется и уточняется на месте экспериментальным путем на разборчивость передаваемых речевых сообщений.

Оповещатели и громкоговорители не должны иметь регуляторов громкости и разъемных соединений.

Коммуникации систем оповещения в отдельных случаях допускается проектировать совмещенными с радиотрансляционной сетью объекта.

4.2 Параметры систем защиты от краж отдельных предметов

Система защиты от краж отдельных предметов должна соответствовать требованиям ГОСТ 32320–2013.

Система защиты от краж отдельных предметов должна состоять из следующих компонентов:

- идентификаторов-меток (включая электронные пломбы), выполненных с использованием любых технологий, и закрепляемых на предметах, подлежащих охране;

- системы обнаружения идентификаторов-меток, которые должны обеспечивать обнаружение метки при ее движении или нахождении в зоне действия системы обнаружения, а так же выдавать специальных сигнал о входе либо при выходе метки из указанной зоны;

- системы мониторинга предметов повышенной опасности.

Система защиты от краж должна обеспечивать возможность выполнение следующих функций:

- обеспечивать дистанционное обнаружение и распознавание предмета с установленным идентификатором-меткой при появлении её в зоне контроля;

- выдавать специальный сигнал при входе или выходе идентификатора-метки из зоны контроля либо ее разрушении (неисправности) с учетом последнего сигнала обмена информации с ней;

- обеспечивать мониторинг предметов повышенной опасности.

Идентификаторы-метки должны:

- выполняться в такой конструкции, которая позволяет их установку (закрепление) на охраняемый предмет без нарушения его целостности, за исключением индентификаторов-меток, которые используются для скрытого маркированию предметов повышенной опасности при условии сохранения в целостности их основных частей (для огнестрельного оружия);

- содержать информацию, достаточную для идентификации предмета, а в случаях, когда законодательством Российской Федерации предмет подлежит обязательному номерному учету – для индивидуальной идентификации такого предмета;

- обеспечивать для предметов повышенной опасности (оружия, основных частей огнестрельного оружия) хранение в электронных идентификаторах-метках, санкционированное изменение и обмен информацией об индивидуальном учете данных предметов.

Электронные идентификаторы-метки, устанавливаемые на упаковку (тару) с предметами повышенной опасности, также должны хранить информацию о количестве, виде, типе, моделях помещенных в нее таких предметах и их индивидуальных номерах.

5 Выбор ИСБ для оборудования объектов

В основе принципа выбора ИСБ должно лежать достижение максимальной эффективности защиты объекта, которая определяется способностью системы противостоять действиям нарушителей в отношении объектов, их критических элементов, с учетом криминальных угроз, определённых на этапе проведения анализа уязвимости объекта.

При выборе ИСБ для оборудования конкретных объектов, необходимо исходить из предполагаемых принципов охраны объекта и внутриобъектовых зон. Следует учитывать, что состав и степень интеграции конкретной системы будет значительно влиять на ее эффективность функционирования, определяемую такими факторами, как:

- обеспечение установленного на объекте режима доступа;
- степень противостояния проникновению на охраняемый объект нарушителей;
- возможность и качество дистанционного контроля за состоянием и изменениями в охраняемой зоне;
- степень противостояния совершению несанкционированных, в том числе криминальных, действий;
- степень достоверности информации о попытках нарушений или несанкционированных действиях;
- соответствие степени угрозы уровню применяемых технических средств для каждого участка охраняемого объекта;
- обеспечение необходимого уровня защиты информационных каналов ИСБ;
- общая организация деятельности служб охраны и безопасности;
- возможность пресечения нарушений и несанкционированных действий, проведение превентивных мероприятий по их недопущению;
- оперативность реагирования на попытки совершения нарушений и несанкционированных действий.

При построении ИСБ объекта также необходимо руководствоваться следующими принципами, упрощающим установку всех элементов системы, их обслуживание, а также положительно сказывающимися на соотношении стоимость/качество:

- адекватности криминальным угрозам;
- зонального построения;
- равнопрочности;
- адаптивности.

Принцип адекватности криминальным угрозам: принятые на объекте организационные меры и технические способы реализации защиты объектов и их элементов должны соответствовать криминальным угрозам, определенным на этапе проведения анализа уязвимости объекта.

Зональный принцип: ИСБ объекта должна предусматривать возможность создание отдельных охраняемых зон и зон ограниченного доступа.

Критические элементы объекта должны размещаться в соответствующих охраняемых зонах в соответствии с установленными для них уровнями защищенности. При определении границ отдельных охраняемых зон объекта должно обеспечиваться усиление защиты от периферии к центру, то есть к критическим элементам, определяющим категорию объекта. Если в процессе проведения оценки эффективности системы противокриминальной защиты выясняется, что существующих охраняемых зон недостаточно для нейтрализации потенциальных угроз, то возможна реализация дополнительных охраняемых рубежей защиты внутри существующих зон.

Принцип равнопрочности: требуемый уровень эффективности ИСБ должен быть обеспечен для всех видов криминальных угроз, выявленных в процессе анализа уязвимости объекта.

Требуемый уровень эффективности защиты должен учитывать особенности критических элементов и критерия

«эффективность/стоимость».

Принцип адаптивности: работа ИСБ не должна создавать препятствий функционированию объекта и должна быть адаптирована к технологическим особенностям его работы, в том числе в чрезвычайных ситуациях, с учетом принятых на объекте мер технологической и пожарной безопасности.

Выбор состава оборудования ИСБ следует начинать с анализа предъявляемых к системе функциональных требований, проведения мероприятий по обследованию объекта и определения возможности и методов реализации выбранных технических решений.

При обследовании объекта необходимо определить:

- характеристики значимости его помещений;

- строительные и архитектурно-планировочные решения;

- материалы исполнения строительных конструкций объекта и отделки внутренних помещений;

- наличие и особенности работы штатных инженерно-технических коммуникаций;

- условия эксплуатации и режимы работы помещений;

- ограничения или расширения права доступа отдельных сотрудников;

- параметры установленных или предполагаемых к установке на данном объекте ТС ИСБ.

По результатам обследования определяются тактико-технические характеристики и структура ИСБ и предоставляются исходные данные для составления технического задания на оборудование объекта.

В техническом задании указывается:

- назначение ИСБ, техническое обоснование и описание системы;

- состав ИСБ;

- размещение компонентов ИСБ;

- условия эксплуатации ТС ИСБ;

- основные технические характеристики ТС ИСБ;

- требования к маскировке и защите ТС ИСБ от вандализма;

- требования к оповещению о тревожных и аварийных ситуациях и принятие соответствующих мер по их пресечению или предупреждению;

- возможность работы и сохранения данных без компьютера или при его отказе;

- алгоритм работы ИСБ в аварийных и чрезвычайных ситуациях;

- ПО ИСБ;

- требования к безопасности;

- требования к электропитанию;

- требования к обслуживанию и ремонту ИСБ.

При наличии агрессивных условий эксплуатации: вне закрытых отапливаемых помещений, помещений с повышенным содержанием пыли, влажности воздуха, низкой или высокой температурой, взрывоопасной средой следует ориентироваться на специализированные ТС ИСБ, предназначенные для работы в особых условиях. Для надежной работы подсистем ИСБ на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения электропитания, удаленность компонентов от управляющего центра, заземление ТС ИСБ и т. д.

При интеграции элементов ИСБ следует учитывать ряд факторов, в значительной мере влияющих на удобство эксплуатации при выполнении оперативных задач, надежность их совместной работы, удобство и скорость проведения работ по техническому обслуживанию и ремонту:

- возможность максимальной синхронизации всех компонентов ИСБ;

- возможность интеграции на программном, аппаратном и релейных уровнях;

- возможность организации линий связи посредством стандартных интерфейсов;

- стремление к реализации схемотехнических решений с единым состоянием сигнальных выходов ИСБ во всех используемых режимах.

При требуемом уровне охраны объекта, техническая, программная, информационная и эксплуатационная совместимость элементов ИСБ характеризуется единством функций и технических характеристик, при:

- взаимодействии всех ТС ИСБ;
- возможности совместной работы нескольких программ и подпрограмм, необходимых при взаимодействии, и возможности обмена данными между ними;
- установлении единого вида, способа хранения, регистрации и отображения информации;
- использовании стандартных наборов аппаратуры, приборов в процессе эксплуатации и технического обслуживания для осуществления контроля работоспособности и ремонта.

6 Проектирование ИСБ объекта

Проектирование ИСБ включает следующие этапы работ:

- проведение анализа уязвимости объекта, оценка эффективности существующей системы (для действующих объектов);

- разработка и утверждение технического задания на проектирование (реконструкцию) ИСБ объекта;

- разработка проектной документации.

Анализ уязвимости объекта и оценка эффективности существующей системы безопасности осуществляется путём проведения комиссионного обследования объекта комиссией, формируемой заказчиком.

В состав комиссии по обследованию объектов принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации включаются представители подразделений вневедомственной охраны.

Итоги комиссионного обследования оформляются актом. В акте обследования должны быть отражены:

- анализ возможных криминальных угроз;

- функциональные и строительные особенности объекта, характер и условия размещения материальных ценностей, радиоактивных, пожаровзрывоопасных и биологических веществ, создающих реальную угрозу возникновения источника кризисной ситуации;

- вид охраны: физическая, техническая, совмещенная (физическая и техническая);

- уязвимые места и строительные конструкции, через которые возможно несанкционированное проникновение на объект;

- охранные и тревожные зоны, рубежи охраны, технические средства обеспечения противокриминальной защиты, подлежащие монтажу, места их установки и меры по маскировке, способы блокировки строительных конструкций и уязвимых мест.

При недостаточной инженерно-технической укрепленности зданий, сооружений, помещений, отдельных строительных конструкций должно оформляться задание по усилению инженерно-технической укрепленности объекта в виде приложения к акту.

Техническое задание на ИСБ объекта разрабатывается на основе акта анализа уязвимости объекта и является обязательным документом для разработки проектной документации при реконструкции, оснащении ИСБ объекта или при проектировании строительства (реконструкции) объекта в целом.

Техническое задание на проектирование системы противокриминальной защиты разрабатывается заказчиком на основании исходных данных на проектирование, предоставляемых представителем подразделения вневедомственной охраны, уполномоченной на проведение данного вида работ в соответствии с действующим законодательством.

К техническому заданию прилагается:

- генеральный план объекта с размещением производственных и административно-хозяйственных зданий, контрольно-пропускных пунктов, зданий караула, центрального пункта управления, размещения рубежей охраны объекта, отдельных локальных зон, расположения на территории объекта подземных и наземных коммуникаций;

- схема дорог для определения маршрутов движения наряда (пешего или автотранспортного) по территории объекта;

- при недостаточной инженерно-технической укрепленности зданий, сооружений, помещений, отдельных строительных конструкций должно оформляться задание по усилению инженерно-технической укрепленности объекта в виде приложения к техническому заданию;

Дополнительные данные для проектирования в составе:

- архитектурно-строительные чертежи зданий и сооружений, подлежащих оснащению проектируемой системой (поэтажные планы, разрезы, фасады);

- чертежи коммуникаций (наземных и подземных, пересекающих периметр объекта);

- технические условия на подключение электронагрузок проектируемой системы;

- отчеты по геологическим изысканиям.

Проектная документация должна содержать следующий комплект документов:

- техническое задание на разработку проекта;

- пояснительную записку (в пояснительной записке к проекту должны быть отражены все требования технического задания);

- рабочую документацию, содержащую планы расположения оборудования, схемы электрические;

- спецификации оборудования и материалов;

- сметную документацию;

- чертежи нестандартизованного оборудования или задания на его разработку;

- эксплуатационную документацию на ИСБ объекта;

- эксплуатационную документацию на технические средства, входящие в состав ИСБ объекта.

Проектная документация согласовывается с подразделением вневедомственной охраны и утверждаются заказчиком.

Обоснованные отступления (изменения, исправления) от проектной документации в процессе монтажа допускаются только при наличии разрешений (согласования) заказчика и соответствующих организаций, участвующих в утверждении и согласовании данных документов.

Разработка документации, содержащей сведения конфиденциального характера, а также ее хранение и доступ к ней осуществляются в соответствии с действующим законодательством с учётом специфики объекта.

7 Ввод в эксплуатацию ИСБ

Прием ИСБ в эксплуатацию производится комиссией, в которую включаются представители:

- заказчика;

- службы охраны объекта;

- монтажной и пусконаладочной организаций;

- подразделения вневедомственной охраны войск национальной гвардии Российской Федерации, осуществляющего охрану объекта;

- при необходимости могут быть привлечены специалисты других организаций и ведомств.

При приемке выполненных работ по монтажу и пусконаладке ИСБ комиссия осуществляет:

- проверку качества выполненных монтажно-наладочных работ и их соответствие проектной документации, а также требованиям технической документации предприятия-изготовителя на ИСБ;

- испытания работоспособности смонтированной ИСБ на соответствие требованиям технического задания.

При обнаружении отдельных несоответствий выполненных работ проектной документации, комиссия составляет акт о выявленных отклонениях, на основании которого организация, проводившая монтаж и пусконаладку, обязана устранить их в срок, установленный комиссией, и вновь предъявить смонтированную ИСБ к сдаче в эксплуатацию.

Смонтированная ИСБ считается принятой в эксплуатацию комиссией, если проверкой установлено:

- оборудование объекта техническими средствами ИСБ выполнено в соответствии с проектной документацией;

- испытания работоспособности ИСБ дали положительные результаты.

При эксплуатации ИСБ необходимо проведение ее технического обслуживания в соответствие с требованиями эксплуатационной документации.

Основные задачи технического обслуживания эксплуатации ИСБ:

- обеспечение бесперебойного функционирования;

- контроль технического состояния ИСБ и определение пригодности к дальнейшей эксплуатации;

- выявление и устранение неисправностей и причин ложных срабатываний, уменьшение их количества;

- ликвидация или недопущение последствий воздействия климатических, производственных и иных факторов, которые могут отрицательно повлиять на эксплуатационные параметры ИСБ;

- проведение ремонта.

Техническому персоналу, осуществляющему эксплуатацию и сопровождение технических средств ИСБ, использующих в качестве основного или резервного источника электропитания автономные элементы электропитания, предлагается проведение следующих мероприятий:

- осуществление входного контроля закупаемых автономных источников электропитания, включающий их визуальный осмотр, проверку сопроводительных документов, замер электрических параметров;

Примечание – Если измеренное значение напряжения на герметизированных свинцово-кислотных АКБ составляет менее 11,2 В, они бракуются и не подлежат закупке.

- обеспечение соблюдения необходимого температурного режима помещения, используемого для хранения АКБ;

Примечание – Помещения, не удовлетворяющие температурному режиму хранения АКБ, указанному в технической документации на конкретные типы АКБ, не могут быть использованы для хранения АКБ!

- осуществление периодического контроля (не реже одного раза в месяц) электрических параметров АКБ, находящихся на хранении.

Примечание – Если измеренное значение напряжения на герметизированных свинцово-кислотных АКБ составляет менее 11,2 В, следует выполнить их заряд продолжительностью не менее 24 часов (значения зарядного напряжения и предельного зарядного тока в буферном режиме заряда, приводятся в технической документации на АКБ).

- осуществление контроля технического состояния и электрических параметров автономных источников электропитания, находящихся в эксплуатации.

Примечание – Эксплуатация неисправных или выработавших свой ресурс автономных элементов электропитания, недопустима.

8 Применение ИСБ на взрывоопасных объектах

8.1 Общие положения

К категории опасных производственных объектов относятся объекты, на которых получаются, используются, перерабатываются, образуются, хранятся, транспортируются, уничтожаются следующие опасные вещества:

- воспламеняющиеся;
- окисляющие;
- горючие;
- взрывчатые;
- токсичные вещества.

В эту категорию попадают и взрывоопасные объекты. Для организации охраны таких объектов (объектов нефтегазового комплекса, складов хранения боеприпасов и взрывчатых веществ, различных объектов химического и мукомольные производства и т.д.) невозможно применение технических средств в обычном исполнении. Оборудование, применяемое для охраны взрывоопасных объектов, должно быть выполнено в специальном взрывозащищенном исполнении.

Действующими нормативными документами в области взрывозащищенного оборудования являются серия стандартов ГОСТ Р 30852.9–2002 (МЭК 60079-10:1995), которые соответствуют требованиям международной электротехнической комиссии и европейским стандартам, а так же 7 раздел ПУЭ.

Взрывозащищенное электрооборудование – это электрооборудование, в котором предусмотрены конструктивные меры по устранению или затруднению возможности воспламенения окружающей его взрывоопасной среды вследствие эксплуатации этого электрооборудования.

Вид взрывозащиты – специальные меры, предусмотренные в электрооборудовании с целью предотвращения воспламенения окружающей взрывоопасной газовой среды; совокупность средств взрывозащиты электрооборудования, установленная нормативными документами.

Группа, к которой должно принадлежать электрооборудование, определяется, исходя из категории взрывоопасной смеси:

I – рудничный метан;

II – остальные промышленные газы и пары.

Технические средства охраны ИСБ относятся к группе II – оборудованию для внутренней и наружной установки (кроме рудничного).

Наибольшее распространение построения взрывозащищенного оборудования технических средств ИСБ получили два вида:

- взрывонепроницаемая оболочка «d»;

- искробезопасная электрическая цепь «i».

Взрывонепроницаемая оболочка основывается на идее сдерживания взрыва, то есть в данном случае допускается возникновение взрыва внутри оболочки, однако ее конструкция гарантирует, что не произойдет распространения взрыва во внешнюю среду. Технические средства ИСБ в этом случае должны быть выполнены с применением этого вида взрывозащиты, провода ШС, интерфейсов и линий электропитания прокладываются в стальных трубах. К числу недостатков относятся высокая стоимость оборудования и монтажа, а также повышенные требования, предъявляемые к регламентному обслуживанию, к преимуществам – потребляемая мощность подключаемых ТС ИСБ не ограничивается.

Искробезопасная электрическая цепь основывается на ограничении энергии в электрической цепи до безопасного уровня, при котором исключается воспламенение или взрыв даже при коротком замыкании цепи или ее обрыве, когда на оборванных контактах появляется

напряжение холостого хода. Недостатком является невозможность создания устройств, требующих большой мощности электропитания, например мощного свето-звукового оповещателя.

Основное преимущество заключается в том, что такие цепи не способны генерировать искру или оказать тепловое воздействие, которое может послужить причиной взрыва. Это в значительной степени облегчает техническое обслуживание и исключает серьезные последствия при ошибках обслуживающего персонала. ТС ИСБ, выполненные с использованием искробезопасной цепи, не требует специального технического обслуживания, связанного с взрывозащитой.

Взрывозащищенные ТС ИСБ должны иметь маркировку взрывозащиты, которая обязательно наносится на корпусах.

В маркировку в указанной ниже последовательности входят:

- знак уровня взрывозащиты электрооборудования (2, 1, 0);

- знак «Ex», указывающий на соответствие электрооборудования стандартам на взрывозащищенное электрооборудование. («Ex» – от английского explosion – взрыв);

- знак вида взрывозащиты («d», «p», «q», «o», «e», «i», «m», «n», «s»);

- знак группы или подгруппы электрооборудования (II, IIA, IIB, IIC);

- знак температурного класса электрооборудования (T1, T2, T3, T4, T5, T6).

В маркировке по взрывозащите могут иметь место дополнительные знаки и надписи, например буквы «X» и «U», в соответствии со стандартами на электрооборудование с отдельными видами взрывозащиты.

Уровень взрывозащиты – степень взрывозащиты электрооборудования при установленных нормативными документами условиях.

Установлены три уровня взрывозащиты электрооборудования:

- электрооборудование повышенной надежности против взрыва – взрывозащищенное электрооборудование, в котором взрывозащита

обеспечивается только в признанном нормальном режиме его работы. Знак уровня – «2Ex»;

- взрывобезопасное электрооборудование – взрывозащищенное электрооборудование, в котором взрывозащита обеспечивается как при нормальном режиме работы, так и при признанных вероятных повреждениях, определяемых условиями эксплуатации, кроме повреждений средств взрывозащиты. Знак уровня – «1Ex»;

- особо взрывобезопасное электрооборудование – взрывозащищенное электрооборудование, в котором по отношению к взрывобезопасному электрооборудованию приняты дополнительные средства взрывозащиты, предусмотренные стандартами на виды взрывозащиты. Знак уровня – «0Ex».

Маркировка вида взрывозащиты:

- взрывонепроницаемая оболочка маркируется буквой «d»;

- искробезопасная электрическая цепь маркируется буквой «i».

Электрооборудование группы II, имеющее виды взрывозащиты «взрывонепроницаемая оболочка» и (или) «искробезопасная электрическая цепь», подразделяется также на три подгруппы, соответствующие категориям взрывоопасных смесей, в соответствии с таблицей 8.1.

Таблица 8.1 – Подгруппы электрооборудования группы II

Знак группы электрооборудования	Знак подгруппы электрооборудования	Категория взрывоопасной смеси, для которой электрооборудование является взрывозащищенным
II	–	IIA, IIB и IIC
	IIA	IIA
	IIB	IIA и IIB
	IIC	IIA, IIB и IIC

Это распределение базируется на безопасном экспериментальном максимальном зазоре оболочек или минимальном токе воспламенения для электрооборудования с искробезопасными цепями.

Электрооборудование, промаркированное как IIB, пригодно также для применения там, где требуется электрооборудование подгруппы IIA. Подобным образом, электрооборудование, имеющее маркировку IIC, пригодно также для применения там, где требуется электрооборудование подгруппы IIA или IIB.

Электрооборудование группы II в зависимости от значения предельной температуры подразделяется на шесть температурных классов, соответствующих группам взрывоопасных смесей, где предельная температура – наибольшая температура поверхностей взрывозащищенного электрооборудования, безопасная в отношении воспламенения окружающей взрывоопасной среды, в соответствии с таблицей 8.2.

Таблица 8.2 – Температурные классы электрооборудования группы II

Знак температурного класса электрооборудования	Предельная температура, °С	Группа взрывоопасной смеси, для которой электрооборудование является взрывозащищенным
T1	450	T1
T2	300	T1, T2
T3	200	T1 – T3
T4	135	T1 – T4
T5	100	T1 – T5
T6	85	T1 – T6

Для того чтобы установить, какой уровень взрывозащиты должны иметь ТС ИСБ необходимо определить класс взрывоопасной зоны. Согласно п. 7.3.38 ПУЭ, класс взрывоопасной зоны должен определяться

технологами совместно с электриками проектной или эксплуатирующей организации.

Классификация взрывоопасных зон определена в пп. 7.3.40 – 7.3.46 ПУЭ и зависит от концентрации, химических свойств огнеопасных веществ и их агрегатного состояния (газ, пар, жидкость или пыль). Класс взрывоопасной зоны также зависит от того, определено ли присутствие огнеопасных веществ нормальным режимом работы, или это возможно только в результате аварий или неисправностей.

Исходя из класса взрывоопасной зоны, в которой должны устанавливаться ТС ИСБ, определяется требуемый уровень взрывозащиты оболочки или искробезопасной электрической цепи. Различие между этими уровнями заключаются в степени надежности этой цепи. Так, цепи уровня «ia» не должны вызывать воспламенения взрывоопасной смеси даже при двух повреждениях, цепи уровня «ib» при одном повреждения, а цепи уровня «ic» не допускают таких повреждений.

С видом взрывозащиты «взрывонепроницаемая оболочка» выпускается извещатель для работы в подсистеме СОС – ИО 209-22 «СПЭК-11», уровень взрывозащиты «взрывобезопасный», маркировка взрывозащиты 1ExdIIBT5X. Внешний вид извещателя ИО 209-22 «СПЭК-11» приведен на рисунке 8.1.

Рисунок 8.1 – Извещатель ИО 209-22 «СПЭК-11»

Этот извещатель предназначен для применения в неагрессивных средах во взрывоопасных зонах помещений классов 1 или 2 по

ГОСТ Р 30852.9–2002 (МЭК 60079-10:1995) (классы В-Iа, В-Iб, В-Iг по гл. 7.3 ПУЭ).

Электропитание извещателя осуществляется от стационарной искроопасной цепи источника питания ограниченной мощности с разделительным трансформатором, в котором входная и выходная обмотки электрически не связаны между собой и между ними имеется двойная или усиленная изоляция. Выходные контакты «ТРЕВОГА» обеспечивают коммутацию постоянного тока до 30 мА при напряжении до 42 В и могут подключаться к любым приемо-контрольным приборам, обеспечивающим такие параметры в шлейфе сигнализации.

Кронштейн для юстировки включен в комплект поставки извещателя.

Технические характеристики извещателя ИО 209-22 «СПЭК-11» представлены в таблице 8.3.

Таблица 8.3

Характеристика	Значение
Дальность действия, м при коэффициенте запаса	125 25
Напряжение питания, В	от 10 до 27
Чувствительность, мс	130
Длительность извещения «Тревога», с, не менее	2
Диапазон рабочих температур, °С	От минус 40 до плюс 35
Габариты БИ, БП, мм (без учета кронштейна и кабеля в металлорукаве)	155×95×85
Масса, кг	5

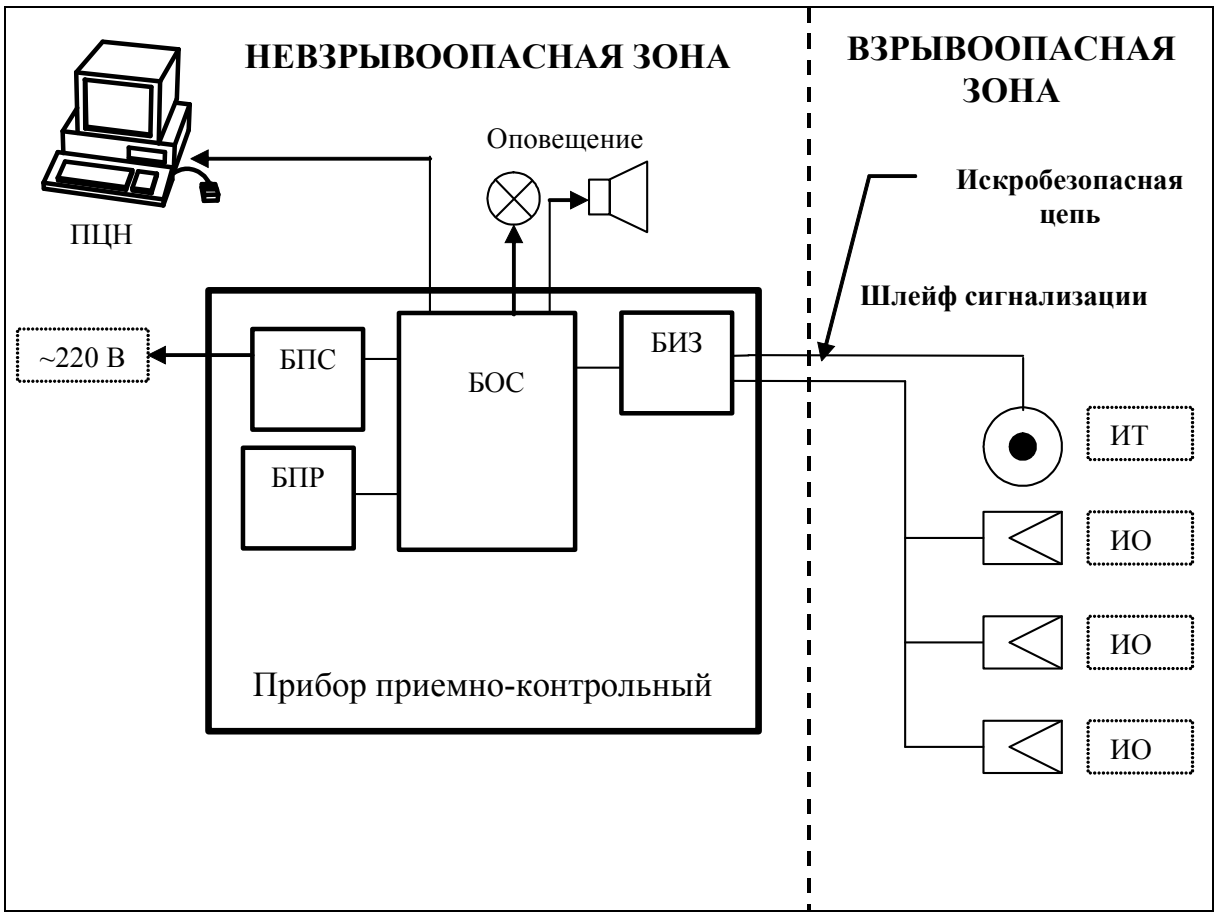
К блокам излучателя и приемника извещателя присоединен кабель в металлорукаве длиной 10 м. Все соединения производятся вне взрывоопасной зоны, во взрывоопасной зоне устанавливаются только указанные блоки.

Вид взрывозащиты «взрывонепроницаемая оболочка» не позволяет получить извещатели, основанные на других физических принципах обнаружения. Некоторые из таких извещателей возможно реализовать с помощью вида взрывозащиты «искробезопасная электрическая цепь».

Формирование искробезопасной цепи выполняется с помощью блоков искрозащиты. Эти блоки могут выполняться как самостоятельные устройства и устанавливаться во взрывобезопасной зоне. Основное достоинство самостоятельных блоков и устройств искрозащиты заключается в том, что они могут быть применены практически к любым ТС ИСБ. Но в этом случае ТС ИСБ, устанавливаемые во взрывоопасной зоне (извещатели, оповещатели и т.д.), должны также выполняться с таким же видом взрывозащиты и должны быть строго согласованы по искробезопасным параметрам

При установке ТС ИСБ во взрывоопасных зонах недостаточно ограничиться выбором взрывозащищенных изделий. Необходимо учитывать возможные суммарные емкость и индуктивность интерфейсов в целом, которые определяются не только собственными емкостью и индуктивностью ТС ИСБ, но и параметрами кабельной трассы, т. е. погонными значениями емкости и индуктивности конкретного типа кабеля и его протяженностью. Эти величины не должны превышать предельных значений, указанных на его корпусе и в паспорте.

Пример оборудования объекта с взрывоопасными зонами приведен на рисунке 8.2



ПЦН – пульт централизованного наблюдения;

БПС – блок питания сетевой;

БПР – блок питания резервный;

БОС – блок обработки сигналов;

БИЗ – блок искрозащиты;

ИТ – извещатель тревожный

ИО – извещатели охранный.

Рисунок 8.2 – Оборудование объекта с взрывоопасными зонами

8.2 СОС для организации охраны взрывоопасных зон помещений с неагрессивной средой

Примером данной СОС является подсистема «Ладога-Ех» в составе ИСБ «Ладога-А». Подсистема «Ладога-Ех» передает информацию о состоянии зон охраны и составных частей в центральный блок «Ладога-А» по двухпроводной линии связи.

В состав подсистемы входят:

- блок расширения шлейфов сигнализации «БРШС–Ех», обеспечивающий питание и прием извещений от извещателей, установленных во взрывоопасной зоне по искробезопасным шлейфам;
- извещатель охранный оптико-электронный объемный ИО 409-40 «Фотон-18»;
- извещатель охранный оптико-электронный линейный ИО 209-30 «Фотон-18А»;
- извещатель охранный оптико-электронный поверхностный ИО 309-18 «Фотон-18Б»;
- извещатель охранный оптико-электронный поверхностный ИО 309-21 «Фотон-Ш-Ех»;
- извещатель охранный поверхностный звуковой ИО 329-9 «Стекло-Ех»;
- извещатель охранный поверхностный вибрационный ИО 313-6 «Шорох-Ех»;
- извещатель охранный точечный магнитоконтактный ИО 102-33 «МК-Ех»;
- сигнализатор тревожный газовый «СТГ-Ех»;
- сигнализатор тревожный затопления «СТЗ-Ех».

Внешний вид блока расширения шлейфов сигнализации «БРШС-Ех» приведен на рисунке 8.3.

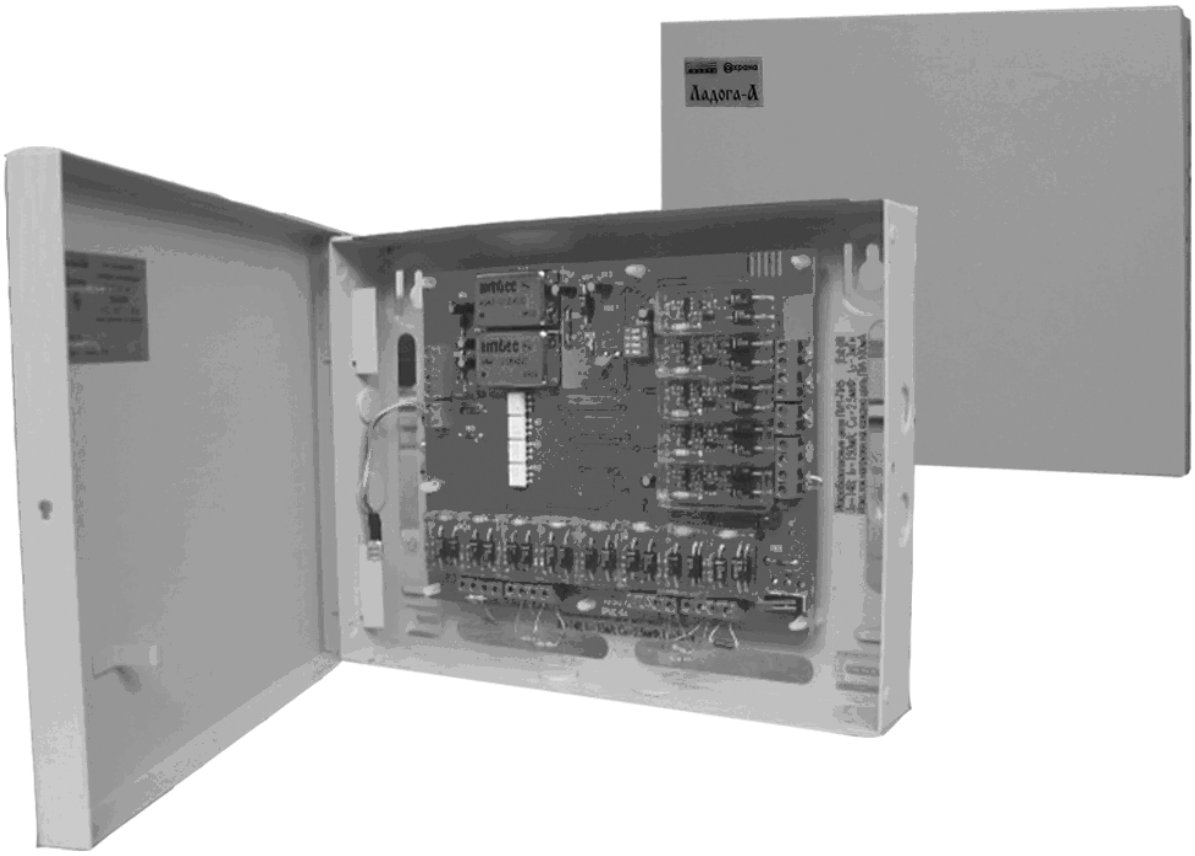


Рисунок 8.3

Блок устанавливается вне взрывоопасной зоны и обеспечивает:

- контроль состояния восьми искробезопасных шлейфов;

- электропитание извещателей напряжением 12 В по искробезопасным цепям;

- отключение электропитания ШС, находящихся в состоянии «КЗ»;

- имитостойкость ШС в составе системы;

- контроль вскрытия корпуса.

Блок «БРШС-Ех» имеет два исполнения в зависимости от номинальной нагрузочной мощности цепей электропитания. Электропитание блока «БРШС-Ех» осуществляется от резервированного источника электропитания номинальным напряжением 12 В («Ладога БП-А»).

Технические характеристики блока «БРШС-Ех» представлены в таблице 8.4.

Таблица 8.4

Характеристика	Значение
Маркировка взрывозащиты	[Exib]IIBX
Напряжение питания, В	от 10,5 до 14
Ток потребления, мА не более (при отсутствии подключенных извещателей к клеммам питания)	150
Параметры цепей электропитания - номинальное выходное напряжение, В - номинальный выходной ток, мА (исп. 1) - номинальный выходной ток, мА (исп. 2)	 12 625 200
Диапазон рабочих температур, ◦С	от плюс 1 до плюс 50
Габариты, мм	230×177×50
Масса, кг	1,5

Извещатели охранные оптико-электронные ИО 409-40 «Фотон-18», ИО 209-30 «Фотон-18А», ИО 309-18 «Фотон-18Б»

Внешний вид извещателей охранных оптико-электронных ИО 409-40 «Фотон-18», ИО 209-30 «Фотон-18А», ИО 309-18 «Фотон-18Б» приведен на рисунке 8.4.

Рисунок 8.4

Данные извещатели предназначены для обнаружения проникновения в охраняемое пространство взрывоопасных зон закрытого помещения.

Особенность – три зоны обнаружения формируются тремя типами линз Френеля:

- объемная – ИО 409-40 «Фотон-18»;
- линейная – ИО 209-30 «Фотон-18А»;
- поверхностная – ИО 309-18 «Фотон-18Б».

Технические характеристики извещателей ИО 409-40 «Фотон-18», ИО 209-30 «Фотон-18А», ИО 309-18 «Фотон-18Б» представлены в таблице 8.5.

Таблица 8.5

Характеристика	Значение
Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания, В	от 9 до 14
Ток потребления, мА	не более 20
Дальность действия (зона обнаружения), м ИО 409-40 «Фотон-18» ИО 209-30 «Фотон-18А» ИО 309-18 «Фотон-18Б»	 12 (объемная) 20 (линейная) 15 (поверхностная)
Габаритные размеры, мм	105×75×56
Масса, кг	не более 0,1
Степень защиты оболочки	IP41
Диапазон рабочих температур, °С	от минус 30 до плюс 50

Извещатель охранный поверхностный оптико-электронный ИО 309-21 «Фотон-Ш-Ех»

Внешний вид извещателя поверхностного оптико-электронного ИО 309-21 «Фотон-Ш-Ех» приведен на рисунке 8.5.

Рисунок 8.5

Данный извещатель предназначен для обнаружения проникновения в охраняемое пространство взрывоопасных зон закрытого помещения.

Особенности:

- сплошная зона обнаружения типа «занавес»,

- рекомендуемая высота установки от 2,5 до 5 м.

Технические характеристики извещателя ИО 309-21 «Фотон-Ш-Ех» представлены в таблице 8.6.

Таблица 8.6

Характеристика	Значение
Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания, В	от 9 до 14
Ток потребления, мА	не более 20
Габаритные размеры, мм	91×52×56
Масса, кг	не более 0,2
Степень защиты оболочки	IP41
Диапазон рабочих температур, °С	от минус 30 до плюс 50

Извещатель охранный поверхностный звуковой ИО 329-9 «Стекло-Ех»

Внешний вид извещателя охранного поверхностного звукового ИО 329-9 «Стекло-Ех» приведен на рисунке 8.6.

Рисунок 8.6

Предназначен для обнаружения разрушения обычного, закаленного, армированного, узорчатого, трехслойного (триплекс), покрытого защитной полимерной пленкой, а также стеклоблоков во взрывоопасных зонах помещений.

Особенности:

- возможность регулировки чувствительности;

- выбор алгоритма работы в зависимости от вида охраняемых стекол и принятой тактики охраны на объекте;

- световая индикация состояния извещателя и помеховой обстановки внутри охраняемого помещения с возможностью отключения индикации.

Технические характеристики извещателя ИО 329-9 «Стекло-Ех» представлены в таблице 8.7.

Таблица 8.7

Характеристика	Значение
Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания, В	от 9 до 14
Ток потребления, мА	30

Продолжение таблицы 8.7

Характеристика	Значение
Максимальная дальность действия, м	6
Диапазон рабочих температур, °С	от минус 20 до плюс 45
Габариты, мм	80×80×35
Масса, кг не более	0,12

Извещатель охранный поверхностный вибрационный ИО 313-6 «Шорох-Ех»

Внешний вид извещателя охранного поверхностного вибрационного ИО 313-6 «Шорох-Ех» приведен на рисунке 8.7.

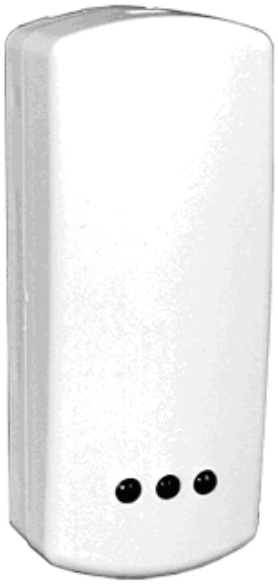


Рисунок 8.7

Данный извещатель предназначен для обнаружения преднамеренного разрушения строительных конструкций в виде бетонных, кирпичных стен и перекрытий, конструкций из дерева, фанеры, ДСП, металлических сейфов и шкафов во взрывоопасных помещениях.

Особенности:

- расширенный диапазон обнаруживаемых воздействий, включая газорежущее, электрорежущее, электродуговое воздействия;

- автоматический выбор алгоритма работы микропроцессора в зависимости от вида разрушающего воздействия;

- три режима тестирования, позволяющих произвести регулировку чувствительности для трех групп инструментов при установке на объекте;

- световая индикация состояния извещателя и помеховых вибраций охраняемой конструкции.

Технические характеристики извещателя ИО 313-6 «Шорох-Ех» представлены в таблице 8.8.

Таблица 8.8

Характеристика	Значение
Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания, В	от 9 до 14
Ток потребления, мА	20
Диапазон рабочих температур, °С	от минус 30 до плюс 50
Габариты, мм	105×45×35
Масса, кг не более	0,3

Извещатель охранный точечный магнитоконтактный ИО 102-33 «МК-Ех»

Внешний вид извещателя охранного точечного магнитоконтактного ИО 102-33 «МК-Ех» приведен на рисунке 8.8.

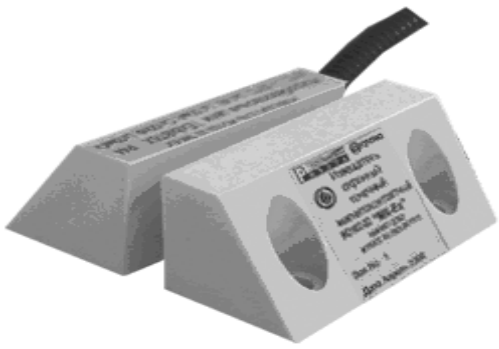


Рисунок 8.8

Данный извещатель предназначен для блокировки на открывание подвижных элементов строительных конструкций (дверей, окон, люков и т.п.), выполненных из конструктивных магнитопроводящих (стальных) или магнитонепроводящих (алюминиевых, деревянных, пластиковых) материалов. Имеется два конструктивных исполнения.

Технические характеристики извещателя ИО 102-33 «МК-Ех» представлены в таблице 8.9.

Таблица 8.9

Характеристика	Значение
Маркировка взрывозащиты	1ExibIIBT6X
Ток коммутации, мА	от 0,1 до 100
Напряжение коммутации, В	от 0,1 до 72
Масса, кг: - магнитоуправляемого датчика - задающего элемента	 0,23 0,15
Степень защиты оболочки	IP44
Диапазон рабочих температур, °С	от минус 10 до плюс 50
Габариты, мм	105×45×35

Сигнализатор тревожный газовый «СТГ-Ех»

Внешний вид сигнализатора тревожного газового «СТГ-Ех» приведен на рисунке 8.9.

Рисунок 8.9

Данный сигнализатор предназначен для обнаружения опасной концентрации в воздухе горючих газов (метана), используемых при отоплении зданий и помещений при индивидуальной и многоэтажной застройке или в котельных.

Технические характеристики сигнализатора «СТГ-Ех» представлены в таблице 8.10.

Таблица 8.10

Характеристика	Значение
Маркировка взрывозащиты	[Exib]BT6X
Напряжение питания, В	от 10 до 13
Ток потребления, мА	не более 50
Габаритные размеры, мм	80×80×35
Масса, кг не более	0,1
Степень защиты оболочки	IP30
Диапазон рабочих температур, °С	от минус 30 до плюс 50

Сигнализатор тревожный затопления «СТЗ-Ех»

Внешний вид сигнализатора тревожного затопления «СТЗ-Ех» приведен на рисунке 8.10.

Рисунок 8.10

Сигнализатор тревожный затопления «СТЗ-Ех» предназначен для обнаружения утечек воды из водопроводов, используемых при водоснабжении и отоплении зданий и помещений при индивидуальной и многоэтажной застройке или в котельных.

В состав сигнализатора «СТЗ-Ех» входит блок обработки сигналов и до трех датчиков затопления.

Технические характеристики сигнализатора «СТЗ-Ех» представлены в таблице 8.11.

Таблица 8.11

Характеристика	Значение
Маркировка взрывозащиты	[Exib]BT6X
Напряжение питания, В	от 9 до 14
Ток потребления, мА не более	10
Габаритные размеры, мм блок обработки сигналов датчик затопления	 80×80×35 35×15×15

Продолжение таблицы 8.11

Характеристика	Значение
Масса, кг не более блок обработки сигналов датчик затопления	 0,08 0,007
Степень защиты оболочки	IP40
Диапазон рабочих температур, °С	от минус 30 до плюс 50

8.3 Специальные требования при установке технических средств ИСБ во взрывоопасных зонах

ТС ИСБ (за исключением извещателей СОС, включаемых в искробезопасные цепи), предназначенные для монтажа во взрывоопасных зонах, должны, в зависимости от классов взрывоопасных зон, иметь исполнение, отвечающее требованиям ПУЭ. При этом взрывозащищенные ТС ИСБ должны по взрывозащите соответствовать категории и группе взрывоопасных смесей, способных образоваться в зоне, и иметь соответствующую маркировку по взрывозащите.

Допускается установка ТС ИСБ во взрывоопасных зонах любого класса при условии, что уровень их взрывозащиты или степень защиты являются более высокими.

Перед монтажом ТС ИСБ, предназначенные для установки во взрывоопасных зонах, другие ТС ИСБ, искробезопасные цепи которых заходят во взрывоопасные зоны, должны быть тщательно осмотрены с целью проверки наличия маркировки по взрывозащите, предупредительных надписей, пломб, заземляющих устройств, отсутствия повреждения оболочек.

Не допускается устанавливать ТС ИСБ с обнаруженными дефектами.

Во взрывоопасных зонах классов В-1 и В-1а должны применяться провода и кабеля с медными жилами. Допускается применение проводов и

кабелей с алюминиевыми жилами во взрывоопасных зонах классов В-16, В-1г, В-II, В-IIа.

Во взрывоопасных зонах любого класса допускается применять:

- провода с резиновой, поливинилхлоридной изоляцией;

- кабели с резиновой, поливинилхлоридной и бумажной изоляцией в резиновой, поливинилхлоридной и металлической оболочках.

Не допускается применение кабелей:

- с алюминиевой оболочкой во взрывоопасных зонах классов В-1 и В-1а;

- полиэтиленовой изоляцией и оболочкой во взрывоопасных зонах любого класса.

Способы прокладки кабелей и проводов во взрывоопасных зонах приводится в таблице 8.12.

Таблица 8.12

Кабели и провода	Способы прокладки	Класс взрывоопасной зоны
Бронированные кабели	Открыто – по стенам и строительным конструкциям на скобах и кабельных конструкциях; в коробах, лотках, на тросах, кабельных и технологических эстакадах; в каналах. Скрыто – в земле (траншеях), в блоках.	В зонах любого класса

Продолжение таблицы 8.12

Кабели и провода	Способы прокладки	Класс взрывоопасной зоны
Небронированные кабели в резиновой поливинилхлоридной и металлической оболочках	Открыто – при отсутствии механических и химических воздействий; по стенам и строительным конструкциям на скобах и кабельных конструкциях; в лотках, на тросах. В каналах пылеуплотненных (например, покрытых асфальтом) или засыпанных песком. Открыто – в коробах. Открыто и скрыто – в стальных водогазопроводных трубах	В-la, В-16. В-1г, В-IIа (кроме силовых сетей и вторичных цепей до 1 кВ) В-II, В-IIа В-la, В-16, В-1г В зонах любого класса
Изолированные провода	То же	То же

При прокладке искробезопасных цепей должны соблюдаться следующие требования:

- искробезопасные цепи должны отделяться от других цепей с соблюдением требований ГОСТ 227825–78, использование одного кабеля для искробезопасных и искроопасных цепей не допускается;

- изоляция проводов искробезопасных цепей должна иметь отличительный синий цвет. Допускается маркировать синим цветом только концы проводов;

- провода искробезопасных цепей должны быть защищены от наводок нарушающих их искробезопасность.

Проходы кабелей сквозь внутренние стены и междуэтажные перекрытия в зонах классов В-1, В-1а и В-II следует выполнять в отрезках водогазопроводных труб. Зазоры между трубами и кабелями должны быть заделаны уплотнительным составом на глубину 100 – 200 мм от конца

трубы, с общей толщиной, обеспечивающей огнестойкость строительных конструкций.

При переходе труб электропроводки из помещения со взрывоопасной зоной класса В-1 или В-1а в помещение с нормальной средой, или взрывоопасную зону другого класса, с другой категорией или группой взрывоопасной смеси, или наружу труба с проводами в местах прохода через стену должна иметь разделительное уплотнение в специально для этого предназначенной коробке.

Допускается установка разделительных уплотнений со стороны невзрывоопасной зоны или снаружи, если во взрывоопасной зоне установка разделительных уплотнений невозможна.

Не допускается использование соединительных и ответвительных коробок для выполнения разделительных уплотнений.

Во взрывоопасных зонах любого класса не допускается устанавливать соединительные и ответвительные кабельные муфты, за исключением искробезопасных цепей.

Вводы кабелей в ТС ИСБ должны выполняться при помощи вводных устройств. Места вводов должны быть уплотнены. Не допускается ввод защитных электроприводов в технические средства, имеющие вводы только для кабелей.

Отверстия в стенах и в полу для прохода кабелей и труб электропроводки должны быть плотно заделаны несгораемыми материалами.

Через взрывоопасные зоны любого класса, а также на расстоянии менее 5 м по горизонтали и вертикали от взрывоопасной зоны не допускается прокладывать транзитные электропроводки и кабельные линии всех напряжений. Допускается их прокладка в трубах, в закрытых коробах, в полах.

9 PSIM (ПСИМ) – системы

На сегодняшний день для осуществления охраны объектов применяется широкий спектр различных систем безопасности, входящих в состав ИСБ. Количество извещателей, видеокамер, датчиков различных дополнительных систем жизнеобеспечения неуклонно растет. В силу этого, для обработки поступающей информации и своевременного реагирования на возникающие угрозы безопасности объектов, требуется привлечение значительных материально-технических и человеческих ресурсов. При этом, последней инстанцией принятия решений о приоритете реагирования на одновременно возникшие угрозы безопасности, является оператор АРМ ИСБ, что из-за влияния «человеческого фактора», далеко не всегда приводи к принятию оптимальных решений. Одним из перспективных путей преодоления данной проблемы является использование технологии машинной (интеллектуальной) обработки данных с предоставлением оператору АРМ ИСБ возможных сценариев принятия решений, а также аппаратно-программная интеграция имеющихся (разнородных) систем безопасности.

Данная технология реализуется с помощью применения интеллектуальных интегрированных цифровых платформ, собирающих и обрабатывающих информацию от различных систем обеспечения безопасности. Такие платформы называются PSIM (ПСИМ) – системы (от английского Physical security information management – «управление информацией о физической безопасности») – категория программного обеспечения, предоставляющая аппаратно-программный комплекс для интеграции нескольких независимо функционирующих систем, программных продуктов и ТС, а также управления ими через единый пользовательский интерфейс.

ПСИМ-система – это интеллектуальная интегрированная цифровая программная платформа, которая собирает и обрабатывает информацию от

разрозненных устройств обеспечения безопасности и информационных систем, после чего складывает ее в одну многомерную мультифизическую обобщенную объемную картинку – среду трехмерных моделей объектов управления и наблюдения. Источниками информации могут быть как базовые, так и дополнительные (вспомогательные) системы ИСБ.

ПСИМ-системы позволяют интегрировать уже функционирующие на объекте системы обеспечения безопасности. Главным преимуществом ПСИМ-систем перед ИСБ является возможность осуществления тотального контроля над ТС каждой из систем безопасности, что позволяет ей формировать полноценную объективную картину текущей обстановки на объекте. Наличие исчерпывающей информации по всем системам, позволяет ПСИМ-системам провести анализ сложившейся на объекте ситуации и предложить оператору оптимальное решение. Также ПСИМ-системы отличаются возможностью использовать открытые протоколы взаимодействия, совместимые с оборудованием различных производителей, что обеспечивает больше возможностей для расширения систем безопасности и может снизить затраты на внедрение за счет более широкого использования существующего оборудования.

Основополагающим принципом организации ПСИМ-системы является способность осуществлять централизованное управление информацией, поступающей от систем безопасности, посредством организации единого ситуационного центра (моноцентрическая модель управления) или многоуровневой структуры таких центров (принцип полицентрического построения систем безопасности), в одном или нескольких диспетчерских (операторских) центров.

К основным составляющим ПСИМ-систем следует отнести несколько логических модулей:

- интеграция;
- аналитика;
- управление.

Такая структура позволяет при возникновении критической или тревожной ситуации, обладая полной информацией, быстро реагировать на события и инциденты, а естественное восприятие обстановки ускоряет и обеспечивает адекватное принятие решения и его корректное воплощение.

К основным функциям ПСИМ-систем следует отнести:

- функцию анализа входного потока событий для исключения создания дубликатов уже обрабатываемых инцидентов. Все события, связанные с одной ситуацией, включаются в один инцидент. Эта функция в значительной степени снижает нагрузку на оператора системы безопасности;

- функцию создания интерактивных пошаговых инструкций по реагированию на инциденты. В систему закладывается ряд пошаговых инструкций. Вместе с тем указанные системы обеспечивают возможность проактивного функционирования. Данная функция реализована на основе анализа имеющейся информации от систем безопасности и последующего прогнозирования событий. Такой подход может позволить свести к минимуму «человеческий фактор» при принятии решений в нештатных ситуациях;

- функцию гибкой цифровой интеграции, объединения с разнообразными существующими и планируемыми системами, без ограничения оборудованием конкретного поставщика. Обычные СОТ или СКУД используют закрытые протоколы. В этом случаяе расширить систему можно только с помощью устройств одного производителя, на основе одного протокола обмена данными. ПСИМ-системы имеют возможность сбора сигналов от систем безопасности на уровне данных.

Также в указанных системах реализуется ситуационно-аналитический подход, позволяющий не только реагировать на случившиеся инциденты путем получения и кросс-анализа разнородных данных, но и управлять предпосылками формирования этих инцидентов на

базе математической модели с помощью обработки больших данных и генерации сценариев поведения и взаимодействия:

- между людьми;

- между оборудованием или машинами;

- перекрестного взаимодействия на уровне «человек – машина» и «машина – человек». ПСИМ-системы призваны, моделировать и прогнозировать случаи наступления того или иного события, действовать проактивно, а также реагировать в соответствии с внутренними регламентами и нормативами.

Для ситуационно-аналитического компонента характерны следующие признаки:

- единая информационная среда;

- единая система тревог;

- единая система оповещения и помощь в принятии эффективных решений;

- единый журнал регистрации событий от всех систем, обеспечивающих бесперебойность работы предприятия;

- единый формат уведомлений и назначения задач ответственному лицу;

- единый подход к выполнению регламентированных задач и многоуровневая архитектура.

Платформа управления, основанная на многоуровневой архитектуре, поддерживает иерархию сотрудников, принимающих решение по разным типам инцидентов. Если задача не выполнена назначенным специалистом в срок или в соответствии с требованиями, она переходит на уровень выше, но не просто в виде тревоги, переходит именно ответственность за принятие решения.

Также в ПСИМ-системах реализуется:

- интеллектуальный анализ данных. Данные от различных источников не просто собираются, но анализируются с целью выявления рисков, сценариев, закономерностей;

- процессный подход, исключающий игнорирование событий, которые должны быть обработаны. Такой подход должен охватывать не только инциденты безопасности, но и плановую деятельность, привлечение и подготовку персонала, работоспособность и обслуживание систем;

- поддержка принятия решений – автоматическое и автоматизированное принятие решений на основе анализа данных, с обучением системы генерации сценариев;

- комплексное отображение больших объемов требуемых функций, пользовательских графических интерфейсов.

Приложение А

(справочное)

Список использованных нормативных документов

ГОСТ 27.003–2016 Надежность в технике (ССНТ). Состав и общие правила задания требований по надежности.

ГОСТ 28195–89 Оценка качества программных средств. Общие положения.

ГОСТ 29322–2014 (IEC 60038:2009) Напряжения стандартные.

ГОСТ 32320–2013 Технические средства и системы защиты от краж отдельных предметов. Общие технические требования и методы испытаний.

ГОСТ 52436–2005 Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний.

ГОСТ 60065–2013 Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности.

ГОСТ 22782.5–78 Электрооборудование взрывозащищенное с видом взрывозащиты «Искробезопасная электрическая цепь». Технические требования и методы испытаний.

ГОСТ Р 50009–2000 Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний.

ГОСТ Р 51241–2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

ГОСТ Р 30852.9–2002 Электрооборудование взрывозащищенное. Часть 10. Классификация взрывоопасных зон.

ГОСТ Р 51558–2014 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

ГОСТ Р 52435–2015 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.

ГОСТ Р 52551–2016 Системы охраны и безопасности. Термины и определения.

ГОСТ Р 52931–2008 Приборы контроля и регулирования технологических процессов. Общие технические условия.

ГОСТ Р 53195.1–2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения.

ГОСТ Р 53560–2009 Системы тревожной сигнализации. Источники электропитания. Классификация. Общие технические требования. Методы испытаний.

ГОСТ Р 54455–2011 (МЭК 62599-1:2010) Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам.

ГОСТ Р 54831–2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний.

ГОСТ Р 57674–2017 Интегрированные системы безопасности. Общие положения.

Правила устройства электроустановок (ПУЭ) 7-е издание (утв. приказом Минэнерго РФ от 8 июля 2002 г. N 204).

ТР ТС 012/2011 Технический регламент таможенного союза «О безопасности оборудования для работы во взрывоопасных средах».

Приложение Б

(справочное)

Перечень информационных материалов, разработанных
ФКУ «НИЦ «Охрана» Росгвардии

Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» (рекомендован решением заседания Технического совета ГУВО Росгвардии).

Р 78.36.002-2010 Рекомендации «Выбор и применение систем охранных телевизионных».

Р 78.36.019-2012 «Рекомендации по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий».

Р 78.36.022-2012 Методическое пособие «Применение радиоволновых и комбинированных извещателей с целью повышения обнаруживающей способности и помехозащищенности».

Р 78.36.027-2012 «Рекомендации по применению тепловизионного оборудования в системах охранного телевидения».

Р 78.36.030-2013 Методические рекомендации «Применение программных средств анализа видеоизображения в системах охранного телевидения в целях повышения антитеррористической защищенности ПЦО подразделений вневедомственной охраны».

Р 78.36.036-2013 «Методическое пособие по выбору и применению пассивных оптико-электронных инфракрасных извещателей».

Р 78.36.042-2014 «Рекомендации по использованию комплекта оборудования для фиксации и передачи видеоинформации с охраняемого объекта на ПЦО».

Р 78.36.044-2014 «Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений».

ТП 78.36.002-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации административное здание».

ТП 78.36.004-2014 Типовой рабочий проект «Система охранного телевидения».

ТП 78.36.005-2014 Типовой рабочий проект «Система контроля и управления доступом. Административное здание».

Р 78.36.049-2015 Рекомендации «Применение оборудования охранных телевизионных систем в условиях ограниченной видимости или других дестабилизирующих факторов».

Р 78.36.050-2015 Методические рекомендации «Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних периметров, дверей, окон, витрин и подступов к отдельным предметам».

Р 78.36.051-2015 Методические рекомендации «Типовые проектные решения оснащения техническими средствами охраны объектов различных категорий, охраняемых подразделениями вневедомственной охраны полиции».

Р 78.36.052-2015 Методические рекомендации «Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесенных к первой категории».

Р 78.36.053-2015 Методические рекомендации «Применение оборудования с использованием защищённых каналов передачи данных, представляемых операторами сотовой связи».

Р 78.36.058-2016 Методические рекомендации «Оценка трудозатрат работ по проектированию, монтажу и пусконаладке технических средств и систем противокриминальной защиты».

Р 064-2017 Методические рекомендации «Выбор и применение технических средств и систем контроля и управления доступом».

Р 068-2017 «Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны огражденных территорий и открытых площадок».

Р 069-2017 «Рекомендации по выбору и применению средств обнаружения проникновения в зависимости от степени важности и опасности охраняемых объектов».

Р 071-2017 Рекомендации «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения».

Р 075-2018 Методические рекомендации «Участие подразделений вневедомственной охраны войск национальной гвардии Российской Федерации в мероприятиях по антитеррористической защищенности объектов различной ведомственной принадлежности».

Р 076-2018 Методические рекомендации «Ложные срабатывания технических средств охранной сигнализации и методы борьбы с ними».

Р 081-2019 Методические рекомедации «Выбор и применение технических средств охраны для защиты объектов культурного наследия Российской Федерации от преступных посягательств».

Р 083-2019 Методические рекомендации «Нормы и правила проектирования систем безопасности на объектах, охраняемых (принимаемых под охрану) подразделениями вневедомственной охраны».

Р 084-2019 «Требования к функциональным свойствам технических средств безопасности на объектах, подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и правила их обязательного подтверждения соответствия установленным техническим требованиям».

Р 085-2019 Методические рекомендации «Правила производства монтажа и технического обслуживания технических средств безопасности на объектах, охраняемых (принимаемых под охрану) подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации, а также порядок контроля за их проведением».

Примечание – Указанные информационные материалы представлены на официальном сайте ФКУ «НИЦ «Охрана» Росгвардии – http://www.nicohrana.ru.