БИБЛИОТЕКА ТЕХНИЧЕСКОГО СПЕЦИАЛИСТА ОХРАНЫ

Министерство внутренних дел Российской Федерации
Главное управление вневедомственной охраны

Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности

Р 78.36.018 - 2011

Москва 2011

gost.e-ecolog.ru

Министерство внутренних дел Российской Федерации
Главное управление вневедомственной охраны

«УТВЕРЖДЕНО»

Начальником ГУВО МВД России
генерал-лейтенантом полиции
В.В. Савичев
20 декабря 2011 года

Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности

Р 78.36.018 - 2011

Москва 2011

Рассмотрены основные характеристики интегрированных систем безопасности, приведена их классификация и принципы построения, технические требования, освещены вопросы обследования объектов, выбора интегрированных систем безопасности и их технических средств, особенностей размещения и монтажа, порядок ввода в эксплуатацию.

Рекомендации предназначены для инженерно-технических работников вневедомственной охраны, ФГУП «Охрана» МВД России и специалистов служб безопасности различных организаций, занимающихся вопросами поставки, проектирования и монтажа интегрированных систем безопасности на объектах.

@ ФКУ НИЦ «Охрана» МВД России, 2011.

ВВЕДЕНИЕ

В последнее время в целях повышения технической оснащенности охраняемых объектов активно внедряются интегрированные системы безопасности (ИСБ). Это связано с тем, что требования к уровню обеспечения безопасности постоянно растут и для их наиболее полного удовлетворения необходимо широко использовать средства автоматизации, автоматизированные системы управления, новые информационные технологии, которые позволяют интегрировать организационные и технические ресурсы для решения этих задач. Данные системы включают в себя: совместно функционирующие систему охранной и тревожной сигнализации, систему пожарной сигнализации и пожаротушения, систему контроля и управления доступом, систему охранную телевизионную, а также ряд дополнительных подсистем, обеспечивающих защиту от различных видов угроз, возникающих на объектах. Область применения ИСБ - обеспечение комплексной безопасности больших, средних и особо важных объектов.

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 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 зон и факторов риска. Оптимальное соотношение людских и технических ресурсов выбирается в соответствии с поставленными задачами и допустимым уровнем возможных угроз.

В настоящих рекомендациях определены требования к аппаратным средствам и программному обеспечению интегрированных систем безопасности, предназначенных для охраны особо важных объектов, требования к подсистемам, входящим в состав интегрированной системы, технические и организационные меры по защите информации в подсистемах, даны предложения по выбору, проектированию, монтажу и вводу в эксплуатацию систем.

При выборе, проектировании и монтаже интегрированной системы для защиты конкретного объекта, наряду с рекомендациями, приведенными в данном издании, предлагается воспользоваться нормативными документами, рекомендациями, руководящими документами и методическими пособиями, список которых дан в разделе 9 «Список действующих нормативных документов в области ИСБ» и разделе 10 «Список рекомендаций, руководящих документов и методических пособий в области ИСБ».

Целью настоящих рекомендаций является оказание помощи подразделениям вневедомственной охраны, ФГУП "Охрана" МВД России и специалистам служб безопасности различных организаций в правильном выборе ИСБ для применения на конкретных объектах.

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Защита информации**: предотвращение или существенное затруднение несанкционированного доступа к информации (базам данных, протоколам информационного обмена и т. д.) интегрированных систем безопасности.

1.2. **Зона доступа**: здание, помещение, территория, транспортное средство, вход и (или) выход которых оборудованы средствами контроля и управления доступом.

1.3. **Зона обнаружения**: часть пространства охраняемого объекта, при перемещении в которой человека (объекта обнаружения) извещатель выдает извещение о проникновении.

1.4. **Идентификатор**: предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и др. устройства).

1.5. **Идентификационный признак**: уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код.

1.6. **Идентификация**: процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией понимают также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

1.7. **Извещатель**: устройство для формирования извещения о тревоге при проникновении или попытке проникновения, или для инициирования сигнала тревоги потребителем.

1.8. **Интегрированная система безопасности (ИСБ)**: система, объединяющая средства охраны и безопасности объекта на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных.

1.9. **Несанкционированный доступ**: доступ субъектов или объектов, не имеющих права доступа.

1.10. **Несанкционированные действия (НСД)**: преднамеренные действия, направленные на нарушение правильности функционирования системы.

1.11. **Объект противокриминальной охраны**: строительная конструкция или ее часть, территория или ее фрагмент, отдельно расположенные предметы или предмет (принадлежность для хранения ценностей или имущества, экспонат, культовый атрибут, развлекательно-игровой реквизит, вещь).

1.12. **Ограничение доступа**: действия, направленные на недопущение доступа субъектов или объектов, не имеющих права доступа.

1.13. **Оповещатель**: техническое средство, предназначенное для светового и/или звукового оповещения людей о возникновении опасности.

1.14. **Оповещатель звуковой**: оповещатель, выдающий звуковые неречевые сигналы.

1.15. **Оповещатель световой**: оповещатель, выдающий световые сигналы.

1.16. **Подсистема защиты от краж отдельных предметов**: совокупность технических средств, предназначенных для обнаружения попытки несанкционированного перемещения отдельных предметов;

1.17. **Пользователь**: субъект, в отношении которого осуществляются мероприятия по контролю доступа

1.18. **Помехоустойчивость**: способность устройства (системы) выполнять свои функции при наличии помех. Помехоустойчивость оценивают интенсивностью помех, при которых нарушение функций устройства еще не превышает допустимых пределов.

1.19. **Прибор приемно-контрольный (ППК)**: техническое средство охранной или охранно-тревожной сигнализации для приема извещений от шлейфов сигнализации (**ШС**) или других приемно-контрольных приборов, преобразования сигналов, выдачи извещений для непосредственного восприятия человеком, дальнейшей передачи извещений и включения оповещателей, а в некоторых случаях и для электропитания охранных извещателей.

1.20. **Пульт централизованного наблюдения (ПЦН)**: самостоятельное техническое средство (совокупность технических средств) или составная часть системы передачи извещений, устанавливаемая в пункте централизованной охраны (пункте установки ПЦН) для приема от приборов приемно-контрольных извещений о проникновении на охраняемые объекты, служебных и

контрольно-диагностических извещений, обработки, отображения, регистрации полученной информации и представления ее в заданном виде для дальнейшей обработки.

1.21. **Пункт централизованной охраны (ПЦО)**: структурное подразделение отдела (отделения) вневедомственной охраны, осуществляющее централизованную охрану объектов с помощью ПЦН и обеспечивающее оперативный выезд групп задержания на охраняемый объект при поступлении с него извещений о срабатывании сигнализации.

1.22. **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.

1.23. **Система охранная телевизионная (СОТ)**: телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной защиты.

1.24. **Система охранной сигнализации (СОС)**: совокупность совместно действующих технических средств для обнаружения несанкционированного проникновения на охраняемый объект, передачи, сбора, обработки и представления информации в заданном виде;

1.25. **Система передачи извещений (СПИ)**: совокупность совместно действующих технических средств для передачи по каналам связи и приема в пункте централизованной охраны извещений о проникновении на охраняемые объекты на них, служебных и контрольно-диагностических извещений.

1.26. **Средства обнаружения проникновения**: техническое средство охранной или тревожной сигнализации для обнаружения проникновения и формирования извещения о проникновении (извещатели).

1.27. **Считыватель**: устройство, предназначенное для считывания (ввода) идентификационных признаков.

1.28. **Техническое средство ИСБ (ТС ИСБ)**: конструктивно законченное устройство, выполняющее самостоятельные функции и входящее в состав интегрированной системы безопасности или одной из подсистем (систем).

1.29. **Устройства преграждающие управляемые (УПУ):** устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (турникеты, шлюзы, проходные кабины, двери и ворота, а также другие подобные устройства).

1.30. **Устройства управляющие (УУ)**: 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.

1.31. **Чувствительность извещателя**: численное значение контролируемого параметра, при превышении которого должно происходить срабатывание извещателя.

2. ПРИНЦИПЫ ИНТЕГРАЦИИ И КЛАССИФИКАЦИИ ИСБ

2.1. В настоящее время в целях повышения технической оснащенности охраняемых объектов активно внедряются ИСБ. Данные системы включают в себя: совместно функционирующие подсистемы (системы) охранной и тревожной сигнализации, пожарной сигнализации и пожарной автоматики, охранного телевидения, контроля и управления доступом, а также ряд дополнительных подсистем, обеспечивающих защиту от различных видов угроз, возникающих на объектах. Область применения ИСБ - обеспечение комплексной безопасности больших, средних и особо важных объектов. Использование ИСБ позволит подразделениям вневедомственной охраны решить на новом качественном уровне задачи по обеспечению безопасности граждан и охраны собственности.

2.2. Наряду с функциями обеспечения безопасности, интегрированные системы, при условии включения в их состав подсистем (систем) автоматизации обслуживания зданий (объектов) (САОЗ) позволяют максимально эффективно решить ряд задач:

- оперативно принимать решения при аварийных и нештатных ситуациях (пожаре, затоплениях, утечках воды, несанкционированном доступе в охраняемые помещения) и обеспечить их своевременную локализацию;

- оптимизировать количество постов охраны и инженерных служб, что существенно сократит расходы на содержание персонала, его обучение и лицензирование, уменьшит влияние субъективного человеческого фактора;

- обеспечить оптимальный режим управления инженерным оборудованием с целью сокращения затрат по использованию энергоресурсов, потребляемых зданием (электроэнергии, тепла, горячей и холодной воды, воздуха и т.д.);

- проводить объективный анализ работы оборудования, действий служб, обслуживающих системы жизнеобеспечения, охраны при нештатных ситуациях за счет автоматического документирования работы оборудования, решений, принимаемых обслуживающим персоналом.

Такие ИСБ принято называть системами **«интеллектуального здания»**.

2.3. Наибольшее применение в нашей стране на объектах, охраняемых подразделениями вневедомственной охраны, нашли следующие системы: **«Орион», «Рубеж», «Кодос-А-20»,** интегрированный комплекс безопасности **«Пахра»** и др.

Эти ИСБ обеспечивают:

- модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты;
- контроль и управление доступом через точки входа (двери, турникеты, шлюзы, шлагбаумы);
- видеонаблюдение и видеорегистрацию тревожных ситуаций;
- управление установками пожарной автоматики;
- управление инженерными системами здания (кондиционирования, отопления, вентиляции, оповещения, аварийной сигнализации);
- защищенный протокол обмена по каналам связи, имитостойкие шлейфы сигнализации;
- возможность использования для взятия под охрану/снятия с охраны дистанционных радиокарт и электронных ключей;
- речевое предупреждение дежурного о тревожных событиях, возможность записи и воспроизведения речевых сообщений;
- отображение состояний зон, разделов, точек доступа, приемно-контрольных приборов, считывающих устройств, видеокамер на графических планах помещений с подробными текстовыми пояснениями;
- разграничение полномочий дежурных, операторов, администраторов за счет многоуровневой системы паролей и возможность подключения биометрических систем ограничения доступа к программам АРМ;
- протоколирование всех событий, происходящих в системе
- развитую диагностику работоспособности всех блоков и устройств системы.

Примечание: *Системы пожарной сигнализации и пожарной автоматики в данных рекомендациях не рассматриваются. Требования к этим системам определены в действующих нормативных документах МЧС России.*

2.4. В состав ИСБ должны входить не менее двух из перечисленных в п. 2.1 подсистем (систем).

2.5. Каждая из подсистем (систем) ИСБ должна удовлетворять требованиям раздела 7 «Требования к ИСБ» настоящих рекомендаций и соответствующих нормативных документов.

2.6. ИСБ должна представлять собой аппаратно-программный комплекс технических средств, обладающих технической, информационной, программной и эксплуатационной совместимостью. В состав технических и программных средств ИСБ могут входить изделия разных производителей.

2.7. Обязательным требованием являются единые технические условия (ТУ) на систему в целом, единые эксплуатационные документы (руководство по эксплуатации (РЭ), паспорт, руководство по работе с программным обеспечением и другие общесистемные эксплуатационные документы).

2.8. Поставка ИСБ заказчику должна производиться от одного производителя системы, который предоставляет гарантию и отвечает за качество всех компонентов. Компоненты ИСБ, входящие в систему, но являющиеся изделиями других производителей, должны быть обозначены в единых ТУ на систему и должны быть оговорены условия их применения в ТУ и РЭ на систему. Эти изделия должны быть изделиями серийного производства, иметь собственные ТУ и эксплуатационную документацию.

2.9. Поскольку в настоящее время нет единой нормативной базы для комплексных систем безопасности, перед заказчиком встает вопрос выбора ИСБ для оснащения своего объекта, что является достаточно трудной задачей в связи с появившимся разнообразием систем. В определенной мере выбору должна помочь классификация систем.

Основным критерием классификации служит - **«количество реализованных основных функций»**. Например, для ИСБ основные функции - охранная сигнализация, тревожная сигнализация, пожарная сигнализация и пожаротушение, контроль и управление доступом, охранное телевидение. Для систем «интеллектуального здания», в которых в качестве подсистемы входит ИСБ, должны быть определены функции управления жизнеобеспечением здания (объекта). Таким образом, классификация по критерию «количество реализованных основных функций» может

помочь выбирать системы, в зависимости от необходимой степени автоматизации объекта, исходя из экономических соображений.

2.10. Следующим критерием, по которым классифицируют ИСБ, это принципы интеграции. Здесь можно выделить следующие уровни интеграции подсистем (систем).

2.10.1. Интеграция на проектном уровне (аппаратная интеграция).

Объединение систем производится на этапе проектирования системы для каждого конкретного объекта. Такая работа проводится проектно-монтажными организациями. Как правило, в этом случае применяются разнородные подсистемы (системы) различных производителей. Объединение (интеграция) этих подсистем (систем) осуществляется путем установки оборудования управления подсистемами (системами) в общем помещении - ПЦО. Взаимодействие между подсистемами осуществляется на уровне операторов подсистем (систем), то есть без автоматизации. 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, хотя имеется ряд монтажных организаций, которые предлагают свои готовые и проверенные проектные решения.

Разновидностью такого типа интеграции является интеграция посредством релейных контактов, для передачи информационных сообщений между отдельными подсистемами (системами) ИСБ.

Достоинством метода является простота оборудования, невысокая стоимость, возможность объединения подсистем (систем) различных производителей.

Среди недостатков:

- ограниченность видов извещений, которыми могут обмениваться подсистемы (системы);

- проблемы с визуализацией событий и состояния системы в целом;

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

2.10.2. Интеграция на программном уровне (или более точно - на программно-аппаратном уровне с приоритетом программной поддержки). В этом случае роль объединения подсистем играет программный пакет, разработанный и поставляемый 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 производителей. Связь с аппаратными средствами осуществляется с помощью стандартных портов ЭВМ.

Существуют два подхода к созданию специализированного программного обеспечения (далее по тексту - ПО) для ИСБ:

1) ПО разрабатывается под собственное оборудование и не позволяет работать с техническими средствами иных производителей («закрытое» ПО);

2) ПО разрабатывается как «открытая» программная оболочка («открытое» ПО), с возможностью подключения оборудования различных производителей.

Подобное построение ИСБ имеет ряд положительных сторон. Это возможность на программном уровне, используя все возможности современных компьютерных технологий, создавать высококачественные многофункциональные программные системы. Возможность интеграции с аппаратными средствами других производителей (при наличии соответствующего драйвера и соответствующих интерфейсов обмена данными в самих применяемых средствах). Построение ИСБ по данному типу требует меньшего количества линий связи между подсистемами (системами), по сравнению с аппаратной интеграцией.

С другой стороны, это порождает и определенные недостатки - необходимость разработки драйверов для каждого применяемого аппаратного средства. При этом не всегда разработчик аппаратного средства 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, фирма разработчик программной системы, поставляя только

свой программный продукт, не может в этом случае в полном объеме гарантировать работу всей системы в целом.

2.10.3. Интеграция на аппаратно-программном уровне. Наиболее распространенный метод построения 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, в одних руках и система как законченный продукт поставляется с полной гарантией производителя. При этом возможно также получить оптимальные экономические показатели.

Недостатком здесь является то, что каждый производитель технических средств предлагает свою оригинальную систему, как правило, не совместимую с другими средствами.

Примеры ИСБ с этим типом интеграции **«Орион», «Рубеж»** и др.

2.11. Принципы интеграции ИСБ.

2.11.1. Современные ИСБ строятся на основе локальных компьютерных сетей и локальных сетей различного уровня сложности, состоящих из специализированных вычислительных устройств - контроллеров.

Сетевые ИСБ строятся в соответствии с концепцией четырех уровней сетевого взаимодействия.

Примерная структура такой системы приведена на рис. 2.1., в которой:

ДТ - Датчик состояния УПУ;

ИО - извещатель охранный;

ИТ - Извещатель тревожный;

ПИ - Преобразователь интерфейсов;

ППК - Прибор приемно-контрольный;

САОЗ - Система автоматизированного обслуживания зданий;

СКУД - Система контроля и управления доступом;

СОС - Система охранной сигнализации;

СОТ - Система охранная телевизионная;

УВИП - Устройство ввода идентификационных признаков;

УУ - Устройство управляющее;

УПУ - Устройство преграждающее управляемое;

ШС - Шлейф сигнализации.

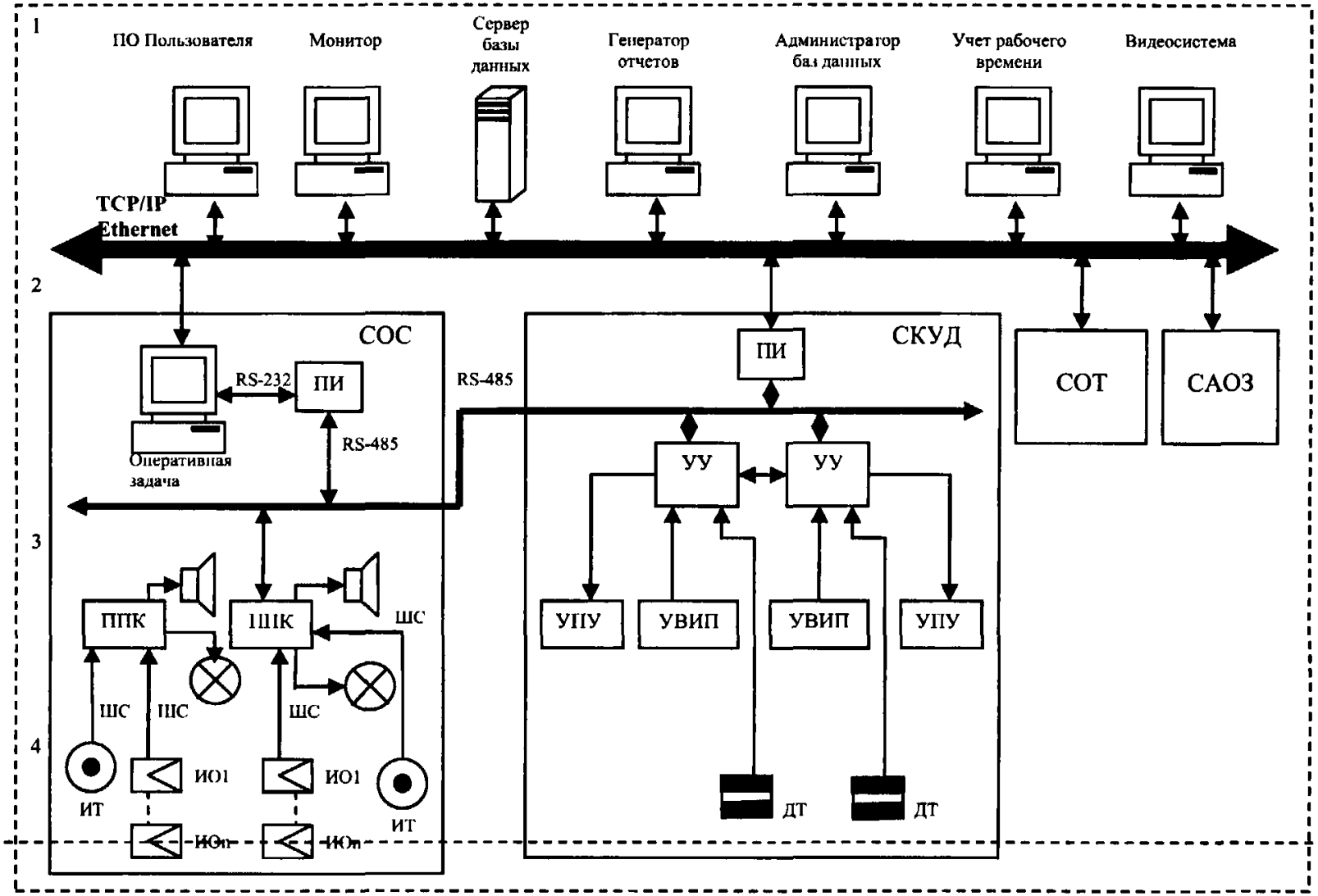


Рис. 2.1. Обобщенная структура ИСБ на основе локальных сетей.

2.11.2. **Первый (высший) уровень** представляет собой компьютерную сеть типа клиент/сервер на основе сети Ethernet, с протоколом обмена TCP/IP и с использованием сетевых операционных систем WindowsNT или Unix -подобных. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов. Выбор операционных систем профессионального класса обусловлен тем, что здесь необходима высокая надежность и защита от несанкционированного доступа.

2.11.3. **Второй уровень** - связь между контроллерами и компьютерами подсистем (вертикальный уровень связи) и связь между однородными контроллерами в каждой из подсистем (горизонтальный уровень связи). На вертикальном уровне наиболее часто используется интерфейс RS-232. На горизонтальном уровне - RS-485 или другие интерфейсы, предназначенные для построения сетей промышленного уровня с хорошей помехозащищенностью и достаточной скоростью обмена данными. В контроллерах некоторых ИСБ возможен прямой выход на первый уровень в протоколе TCP/IP.

2.11.4. **Третий уровень** - связь между контроллерами и считывателями систем доступа. Здесь, как правило, применяется интерфейс RS-485, RS-232 или, ставшие уже стандартом, интерфейсы считывателей Wigand-26. На этом уровне располагаются также средства управления оповещением, адресные блоки управления с релейными и потенциальными выходами.

2.11.5. **Четвертый уровень** - шлейфы контроля состояния извещателей систем охранной, тревожной сигнализаций и входные цепи управления (сбалансированные и несбалансированные радиальные шлейфы, адресные шлейфы, входные цепи для контроля датчиков различных подсистем управления). Как правило, здесь применяются нестандартные специализированные интерфейсы и протоколы.

2.11.6. Среди других общих принципов построения ИСБ можно отметить следующее:

- расширяемая модульная архитектура аппаратных средств (возможность наращивания аппаратных средств);

- для программного обеспечения - возможность добавления модулей и расширения их функций;

- наличие в составе ПО упрощенного специализированного языка программирования для добавления пользователем собственных реализаций взаимодействия компонентов;

- масштабируемость - возможность первоначального развертывания системы в минимальном варианте с последующим наращиванием в процессе эксплуатации, как количественных характеристик, так и функциональных возможностей;

- интеграция подсистем не должна приводить к снижению общей надежности системы и входящих подсистем;

- высокая живучесть системы (сохранение работоспособности системы при выходе из строя отдельных подсистем и блоков, а также сохранение работоспособности в пределах своих функций отдельных подсистем при выходе из строя или потери связи с центром управления);

- автономная работа контроллеров подсистем при нарушении связи с центром управления;

- удаленный доступ с использованием каналов связи для построения территориально распределенных систем;

- для распределенных систем со связью с удаленными компьютерами или с модемной связью, криптографическая защита данных;

- защита программного обеспечения от несанкционированного доступа, разграничение доступа по уровням полномочий пользователей.

3 ТРЕБОВАНИЯ К ИСБ

3.1 Общие положения.

3.1.1. ТС ИСБ предназначены для выполнения следующих задач:

- обнаружение несанкционированного проникновения на охраняемые объекты (здания, помещения, территории, зоны);
- обнаружение несанкционированных действий на охраняемых объектах (зданиях, помещениях, территориях, зонах);
- осуществление контроля и управления доступом персонала и посетителей на охраняемые объекты (здания, помещения, территории, зоны).

3.1.2. В состав ИСБ, в общем случае, должны входить подсистемы (системы) и ТС, предназначенные для выполнения соответствующих функций по обеспечению охраны объекта:

3.1.2.1. Система охранной сигнализации (СОС) в составе:

1) средства обнаружения проникновения - автоматические и неавтоматические (тревожная сигнализация) охранные извещатели;

2) средства сбора и обработки информации - ППК, блоки, устройства и модули;

3) СПИ и ПЦН;

3.1.2.2. СКУД;

3.1.2.3. СОТ.

3.1.2.4. Еще одним компонентом ИСБ, который обязательно присутствует в составе любой из подсистем (систем), является подсистема оповещения. Она присутствует в каждой подсистеме (системе) ИСБ в виде световых и звуковых оповещателей, световых табло, мониторов компьютеров и т.д. Однако в ряде случаев система оповещения может представлять собой отдельную техническую систему, например, систему речевого оповещения, выполненную на основе радиотрансляционной сети и специализированной аппаратуры.

3.1.2.5. В состав ИСБ или подсистемы (системы) СОС может входить подсистема защиты от краж отдельных предметов.

3.1.3. Перечень технических систем, комплексов и средств, составляющих ИСБ, может дополняться при необходи-

мости другими средствами и системами для повышения уровня безопасности охраняемого объекта.

3.1.4. При невозможности объединения отдельных подсистем (систем) в ИСБ допускается самостоятельное развертывание указанных подсистем (систем), однако в этом случае интеграция, с целью повышения эффективности охраны объекта, должна быть обеспечена организационными мерами.

3.1.5. Подсистемы (системы) ИСБ должны обеспечивать:

- возможность непрерывной работы с учетом проведения регламентного технического обслуживания;

- выдачу тревожных сигналов оператору и дежурному составу сил охраны о проникновении или попытках проникновения нарушителей на территорию (с территории) объекта через рубежи охраны и доступа в охраняемые зоны, здания, сооружения, помещения;

- возможность дистанционного наблюдения за состоянием выбранных внутренних и внешних зон охраняемых объектов;

- возможность выполнения установленного режима доступа людей и транспорта на объект, во внутренние зоны, охраняемые здания, сооружения и помещения;

- управление режимами работы подсистем (систем) ИСБ с рабочих мест операторов, наделенных соответствующими полномочиями;

- возможность дистанционного контроля работоспособности периферийной аппаратуры, самотестирования программного обеспечения и аппаратных средств;

- регистрацию и документирование сигналов от средств обнаружения, распоряжений и команд, отдаваемых начальствующим составом сил охраны и службы безопасности, а также сообщений и докладов охранников и командиров тревожных групп сил охраны;

- управление (при помощи средств связи) оперативными действиями личного состава дежурных сил охраны и службы безопасности при выполнении задач по охране и обороне объекта, а также контроль за исполнением команд и приказов;

- защиту программных и аппаратных средств ИСБ от несанкционированного доступа;

- бесперебойное электропитание аппаратуры ИСБ.

3.2. Требования к аппаратным средствам и программному обеспечению ИСБ.

3.2.1. Подсистемы (системы) ИСБ должны обеспечивать необходимую функциональную и аппаратную надежность, пожарную безопасность, помехоустойчивость.

3.2.2. В подсистемах (системах) ИСБ должны использоваться аппаратные средства, которые сертифицированы по безопасности, а также имеют сертификат, подтверждающий основные технические характеристики.

3.2.3. Для создания необходимого уровня безопасности объекта и его персонала допускается применять подсистемы (системы) ИСБ совместно с другими системами (средствами) обеспечения безопасности (пожарной, автоматизации и диспетчеризации технологического оборудования и т.п.). В этом случае функции совместно действующих систем должны дополнять друг друга, не оказывая взаимного мешающего влияния на работоспособность составных частей. В совместно действующих системах должны обеспечиваться: алгоритмическая совместимость и раздельная регистрация поступающих от них служебных и тревожных сигналов.

Условия совместного применения систем должны быть оговорены в техническом задании на проектирование и в эксплуатационной документации.

Приоритетными для выполнения являются требования, обеспечивающие безопасность для жизни людей и пожарную безопасность объекта.

3.2.4. ТС управления и контроля функционирования совместно действующих систем должны определяться их целевым назначением. Предпочтительны автоматические средства управления и контроля, но как дублирующие допускаются и ручные. Целесообразность дублирования определяется требованиями обеспечения эксплуатационной надежности систем. Средства управления и контроля должны иметь защиту от возможных ошибочных действий персонала.

3.2.5. Протоколы обмена информацией и интерфейсы аппаратных средств подсистем ИСБ должны быть стандартных или общепринятых типов и обеспечивать необходимую помехоустойчивость и скорость обмена. Характеристики и параметры

протоколов обмена информацией и интерфейсов должны указываться в технических условиях и эксплуатационной документации на конкретные устройства или системы.

3.2.6. Программно-математическое обеспечение должно обеспечивать совместимость различных подсистем (систем), технических средств ИСБ, а также возможность работы в локальной вычислительной сети.

3.2.7. Программное обеспечение по общим требованиям должно соответствовать ГОСТ 28195-89 и должно быть устойчиво к случайным или преднамеренным воздействиям следующего вида:

1) отключение питания аппаратных средств;

2) программный сброс аппаратных средств;

3) аппаратный сброс технических средств и подсистем;

4) случайное нажатие клавиш на клавиатуре;

5) случайный перебор пунктов меню.

После указанных воздействий и перезапуска программы должна сохраняться работоспособность системы и сохранность установленных данных.

3.2.8. Программное обеспечение должно быть защищено от преднамеренных воздействий с целью изменения установок в системе, несанкционированного копирования и должно обеспечивать резервное сохранение баз данных и системных установок.

3.2.9. Программное обеспечение должно обеспечивать возможность подключения нескольких АРМ и поддерживать функции разделения операторов АРМ подсистем ИСБ по предоставленным полномочиям и назначения индивидуальных прав доступа: просмотр информации, управление системой, администрирование.

3.3. Технические и организационные меры по защите информации ИСБ.

3.3.1. В подсистемах (системах) ИСБ должны быть приняты следующие меры по защите информации:

1) защита аппаратуры подсистем ИСБ от НСД внешних и внутренних нарушителей;

2) защита информации о функционировании подсистем ИСБ от несанкционированного доступа.

3.3.2. Технические меры по защите информации и обеспечению внутренней безопасности подсистем (систем) ИСБ необходимо строить по следующим направлениям:

- ограничение доступа в помещения центральных и локальных пультов управления комплексом ТСО;
- идентификация пользователей системы;
- разграничение прав пользователей по доступу к информации;
- регистрация и учет работы пользователей;
- антивирусная защита и восстановление информации, разрушенной вирусными воздействиями;
- защита информации от аварийных ситуаций;
- кодирование информации;
- контроль вскрытия аппаратуры.

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

- ограничение количества должностных лиц, допущенных к работе с системой;
- размещение ТС в отдельных режимных помещениях;
- разделение функций технического обслуживания и ремонта от основных функций системы;
- периодическая смена паролей для входа в систему.

Перечисленные выше мероприятия дополняются следующими мерами:

- постановкой на учет носителей информации и документации;
- проверкой отсутствия посторонней аппаратуры;
- защитой аппаратуры от электромагнитного излучения и наводок;
- периодической проверкой системы контроля вскрытия аппаратуры.

3.3.4. Программное обеспечение ИСБ должно быть защищено от несанкционированного доступа.

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

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

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

3) третий («системный оператор») - доступ к функциям конфигурации программного обеспечения без доступа к функциям, обеспечивающим управление УПУ СКУД.

Количество знаков в пароле должно быть не менее шести.

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

3.4. Требования к системе охранной и тревожной сигнализации.

3.4.1. На объектах, принимаемых под охрану подразделениями вневедомственной охраны, технические средства охранной и тревожной сигнализации должны удовлетворять "Единым техническим требованиям к системам передачи извещений, предназначенным для применения в подразделениях вневедомственной охраны" и "Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны"

3.4.2. СОС должна:

- обнаруживать действия нарушителя и выдавать извещение о несанкционированном проникновении;

- обеспечивать оперативную подачу сигнала тревоги персоналом объекта (тревожная сигнализация) при возникновении опасной ситуации (нападении и др.);

- выдавать извещение о неисправности при отказе ТС охранной сигнализации;

- не выдавать ложных тревог при переключениях источников электропитания с основного на резервный и обратно.

3.4.3. Средства обнаружения проникновения (охранные извещатели) должны обнаруживать несанкционированное проникновение и/или действия нарушителя с целью проникновения в зону обнаружения. При обнаружении извещатель должен выдавать тревожный сигнал по проводному или беспроводному каналу связи.

3.4.3.1. Охранные извещатели должны иметь следующие функциональные характеристики:

- вид зоны обнаружения (точечная, линейная, поверхностная, объемная, комбинированная);
- размеры зоны обнаружения;
- чувствительность;
- помехоустойчивость;
- вероятность обнаружения.

3.4.3.2. Охранные извещатели (ОИ) должны иметь защиту от несанкционированных действий в целях нарушения их работоспособности.

3.4.4. Средства сбора и обработки информации должны иметь следующие функциональные характеристики:

- информационная емкость - количество контролируемых зон охраны;
-информативность - количество передаваемых (принимаемых) извещений на системы передачи извещений;
- время приема извещения от извещателей (максимально допустимое время контроля всех извещателей, подключенных к прибору);
- параметры контроля состояния канала связи с извещателями (время обнаружения нарушений канала связи, предельные значения параметров линии связи, при которых должен выдаваться сигнал неисправности линии);
- уровень степени защиты от несанкционированного доступа к функции управления взятием/снятием;
- параметры помехозащищенности линии (канала) связи прибора с извещателями;
- параметры и характеристики интерфейса канала связи прибора с СПИ.

3.4.5. СПИ должна обеспечивать передачу извещений (тревожных, служебных, информационных) от охраняемого объекта (от средств сбора и обработки информации) до ПЦН, входящего в состав СПИ.

3.4.5.1. СПИ должна иметь следующие функциональные характеристики:

- вид канала передачи данных от объекта до ПЦН;

- вид и количество передаваемых извещений (извещение о проникновении, извещение о пожаре, служебные и контрольно-диагностические сообщения и другие, если они имеются в системе);

- вид и количество команд для передачи и приема телеуправления (для систем с обратным каналом передачи данных от ПЦН до охраняемого объекта);

- время доставки тревожного извещения;

- приоритеты в передаче тревожных извещений;

- время доставки других видов извещений.

3.4.5.2. По виду канала передачи данных от объекта до ПЦН могут быть использованы следующие каналы связи:

1) выделенные каналы (проводные, оптоволоконные или другие);

2) каналы по линиям телефонной сети общего пользования, в том числе переключаемые, занятые телефонной связью, с использованием частотного выделения служебных сигналов, с использованием аппаратуры автоматического набора номера (информаторные);

3) радиоканал;

4) другие каналы передачи.

Время доставки тревожного извещения для системы передачи извещений должно быть: не более 60 секунд.

СПИ должна обеспечивать контроль канала передачи извещений между охраняемым объектом и ПЦН.

Время обнаружения неисправности канала для СПИ, в зависимости от используемого канала связи, должно быть: не более 120 секунд;

СПИ, имеющая обратный канал передачи данных и предназначенная для работы в автоматическом режиме постановки на охрану и снятия с охраны, должна обеспечить передачу сигнала квитирования на аппаратуру, устанавливаемую на объекте при взятии под охрану и снятии с охраны.

СПИ, при необходимости, должна иметь возможность резервирования канала передачи тревожного извещения.

В СПИ должны быть приняты меры по защите передачи данных в канале передачи от несанкционированного доступа. Вид и методы проверки защиты должны быть указаны в стандартах или технических условиях на СПИ.

3.4.5.3. ПЦН должен обеспечивать:

- приём тревожных извещений о проникновении на охраняемые объекты;

- приём служебных и контрольно-диагностических извещений;

- обработку, отображение, регистрацию полученной информации и представление её в заданном виде для дальнейшей обработки, а также (при наличии обратного канала) для передачи команд телеуправления на объектовое оборудование, установленное на охраняемом объекте;

- управление процессом взятия объектов под охрану и снятие объектов с охраны для систем передачи извещений с ручной тактикой.

3.4.6. Средства тревожной сигнализации представляют собой подсистему охранной сигнализации (или ИСБ) и могут входить в ее состав или могут быть развернуты отдельно, но при этом сигналы тревоги должны передаваться на единый ПЦН.

3.4.6.1. Сигналы тревожной сигнализации должны отличаться от других сигналов.

3.4.6.2. В качестве вызывных устройств тревожной сигнализации 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»: оптико-электронные барьеры; устройства, выполненные в виде предметов, привлекающих внимание нападающих и оснащенных датчиками сигнализации; другие средства аналогичного назначения).

3.4.6.3. Подсистема тревожной сигнализации должна работать по принципу «без права отключения», во время нахождения людей на объекте.

3.4.6.4. Время реагирования (прибытие службы охраны) на сигнал тревожной сигнализации должно быть минимально возможным.

3.4.6.5. Вызывные устройства тревожной сигнализации 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.

3.4.6.6. Ручные и ножные устройства тревожной сигнализации должны размещаться в местах, по возможности незаметных для посторонних.

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

3.5. Требования к системе контроля и управления доступом.

3.5.1. СКУД должна 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;

- выдачу информации на пульт централизованного наблюдения о попытках несанкционированного доступа на объект.

3.5.2. В состав СКУД должны входить:

1) устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;

2) устройства управления (УУ) в составе аппаратных и программных средств;

3) устройства преграждающие управляемые (УПУ) в составе преграждающих конструкций и исполнительных устройств;

4) дополнительные ТС, не являющиеся обязательными элементами системы (аксессуары).

3.5.3. 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 УУ и связь их с зонами доступа (помещениями) и временными интервалами доступа;

- защиту от несанкционированного доступа к программным средствам УУ 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 УУ;

- возможность архивирования базы и просмотра архива в автономном режиме;

- возможность анализировать и вести статистику по рабочему времени сотрудников, проводить анализ нахождения сотрудника на рабочем месте, время переработки (недоработки), опозданий и раннего ухода сотрудника;

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

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

- учет клиентов системы по типу пропусков:

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

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

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

3.5.4. Считыватели УВИП должны обеспечивать:

- считывание идентификационного признака с идентификаторов;

- сравнение введенного идентификационного признака с хранящимся в памяти или базе данных УУ;

- формирование сигнала на открывание УПУ при идентификации пользователя;

- обмен информацией с УУ.

УВИП 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.

3.5.5. УУ должно обеспечивать:

- прием информации от УВИП, 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, УВИП и линий связи.

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

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

2) 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;

3) 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.

3.5.6 Конструктивно СКУД должны строиться по модульному принципу и обеспечивать:

- взаимозаменяемость сменных однотипных ТС;

- удобство технического обслуживания и эксплуатации, а также ремонтопригодность;

- исключение возможности несанкционированного доступа к элементам управления;

- санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

3.5.7. СКУД рекомендуется оборудовать:

- въездную группу (управление шлагбаумом на центральном въезде-выезде, ворота, противотаранные устройства и т. д.);

- турникеты входов в здание;

- кабинеты руководства (входы на VIP-этаж);

- двери выходов из лифтовых холлов;

- служебные входы;

- помещения охраны;

- помещения, в которых непосредственно сосредоточены материальные ценности;

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

- помещения, согласованные с руководителем объекта дополнительно в ходе проектирования.

3.5.8. СКУД должна содержать следующие автоматизированные рабочие места (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.

3.6. Требования к системе охранной телевизионной.

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

3.6.2. СОТ, предназначенная для работы в автоматизированном режиме, применяется в составе ИСБ или в дополнение к системе охранной сигнализации. 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 (дежурному ПЦН) 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.

3.6.3. СОТ, предназначенная для работы в неавтоматизированном режиме, применяется для реального видеонаблюдения за обстановкой на контролируемом объекте (помещении, зоне). В этом случае для работы СОТ требуется организация отдельного поста видеонаблюдения и дежурного оператора видеонаблюдения.

3.6.4. СОТ должна 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.

3.6.5. В состав СОТ должны входить следующие основные составные части:

1) периферийная;

2) каналообразующая;

3) станционная.

3.6.6. 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 видео-

информации 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.

3.6.7. Основные принципы построения СОТ (В соответствии с требованиями ГОСТ Р 51558-2000 и Р 78.36.008-99).

3.6.7.1. Периферийную часть СОТ образуют телекамеры, которые устанавливаются на контролируемых участках территории объекта, в зданиях, сооружениях, помещениях.

Каналообразующая аппаратура обеспечиваст передачу видеосигналов между периферийной и станционной частями и включает в свой состав:

1) линии связи;

2) передатчики видеосигнала;

3) приемники видеосигнала.

В качестве каналов передачи видеосигналов на станционную часть от телекамер, установленных на периметре, могут использоваться как проводные каналы связи - коаксиальные кабели, витая пара, телефонные линии, волоконно-оптические линии и др., так и беспроводные - радиоканал, лазерный или ИК-канал.

В цифровых СОТ для передачи видеосигнала используются стандартные каналы передачи цифровых данных (проводные, оптоволоконные, беспроводные).

Коаксиальный кабель наиболее распространен для передачи видеосигнала и обеспечивает высокое качество, как цветного, так и черно-белого видеосигнала. Максимальная длина

коаксиального кабеля без использования специальных видеоусилителей, как правило - не более 300 м.

Для передачи видеосигнала на расстояния до 1,5 км возможно применение линии передачи «витая пара» с соответствующим оборудованием (передатчиком и приемником) для преобразования видеосигнала в симметричный, поскольку на выходе камеры сигнал не симметричен.

В настоящее время получили распространение системы передачи изображений от телевизионной камеры по телефонным линиям связи, в том числе и по сотовой связи GSM. Основным ограничением таких систем является скорость передачи данных. Максимальная пропускная способность телефонных линий составляет 9600 бод, что позволяет передавать только отдельные кадры.

Высокоэффективную передачу видеосигнала обеспечивают системы передачи по оптоволоконным линиям связи. Передача по оптоволокну имеет следующие преимущества:

- обеспечивает высокую помехозащищенность от электромагнитных помех и полную электрическую изоляцию;
- большие расстояния без промежуточного усиления;
- одновременная передача большого числа нсзависимых сигналов по одному каналу;
- конфиденциальность передаваемой информации.

3.6.7.2. В станционную часть цифровой СОТ входят: видеосерверы, цифровые видеорегистраторы, серверы резервного копирования, пульты видеоконтроля, клавиатуры, мониторы, переключатели консольные, коммутаторы видеосигнала.

Видеосерверы предназначены для сбора, обработки, записи, хранения и передачи в цифровом виде видеоинформации, получаемой от подключенных к ним телекамер, расположенных на территории объекта. Видеосерверы устанавливаются в помещении ПЦО или специально выделенном помещении объекта.

Сервер резервного копирования предназначен для:

программируемой автоматической записи видеоизображений, сохраненных на видеосерверах, на цифровой носитель данных с целью их долговременного хранения;

конвертирования по запросу пользователя видеоизображений, сохраненных на видеосерверах, в нужном формате видеоданных для их записи на сервере резервного копирования.

Пульты видеоконтроля предназначены для отображения информации (видео и данные) о событиях на контролируемой территории объекта и должны обеспечивать:

- предоставление доступа к служебной информации о системе, конфигурирование и параметрирование системы (по паролю);

совместную работу с СОС и СКУД;

- возможность вывода видеоинформации как в полноэкранном, так и в мультиэкранном режимах.

3.6.8. В охране объектов могут применяться системы как черно-белого, так и цветного изображения. Установка той или иной системы зависит от необходимой информативности СОТ, характеристик охраняемого объекта (расположение на местности, освещенность и других признаков) и возможных целей (человек, автомобиль и другие цели).

3.6.9. На объекте СОТ следует оборудовать:

- периметр территории;

- проходные, контрольно-пропускные пункты (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.

3.6.10. Телекамеры, предназначенные для контроля территории объекта или ее периметра, должны работать при температуре окружающего воздуха от минус 40°С до +50°С (от минус 50 - 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.

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.

3.6.11. В СОТ следует использовать обнаружители движения (видеодетекторы), обеспечивающие выдачу сигнала тревоги на ПЦН 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 ПЦН 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.

3.6.12. Вся видеоинформация должна записываться на цифровые видеорегистраторы и храниться, в зависимости от количества записываемых каналов видеоизображения, в течение не менее чем 15 суток.

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.

3.6.13. 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.

3.6.14. Конструктивно СОТ должны 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.

3.7. Требования к подсистемам оповещения.

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

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

1) схему вызова сотрудников, должностными обязанностями которых предусмотрено участие в мероприятиях по предотвращению или устранению последствий внештатных ситуаций;

2) инструкции, регламентирующие действия сотрудников при внештатных ситуациях;

3) планы эвакуации;

4) систему сигналов оповещения.

3.7.3. Подсистемы оповещения должны обеспечивать возможность выполнения следующих функций:

- приоритетную подачу звуковых, речевых, световых (в зависимости от конкретного исполнения) сигналов операторам ИСБ, дежурным службы безопасности объекта;

- подачу сигналов в здания, помещения, на участки территории объекта с постоянным или временным пребыванием людей;

- 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.

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

3.7.5. 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.

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

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

3.8. Требования к подсистеме защиты от краж отдельных предметов.

3.8.1. Подсистема 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.

3.8.2. Подсистема защиты от краж отдельных предметов должна состоять из следующих компонентов:

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

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

3) системы мониторинга предметов повышенной опасности.

3.8.3. 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 скрытой маркировки 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.

3.9. Требования к электромагнитной совместимости.

3.9.1. ТС ИСБ в зависимости от устойчивости к воздействию электромагнитных помех должны иметь следующие степени жесткости по ГОСТ Р 50009:

- первая или вторая степень - при нормальной устойчивости (жилые и офисные помещения);

- третья степень - при повышенной устойчивости (производственные помещения);

- четвертая степень - при высокой устойчивости (помещения с высоким уровнем электромагнитных помех).

Требования по устойчивости к искусственно создаваемым электромагнитным помехам предъявляются к устройствам, имеющим степень жесткости не ниже второй, и устанавливаются в технических условиях на технические средства ИСБ конкретного типа.

3.9.2. Уровень допустимых помех при работе технических средств ИСБ должен соответствовать ГОСТ Р 50009.

3.10. Требования к надежности.

3.10.1. На ТС и подсистемы (системы) ИСБ конкретного типа устанавливают следующие показатели надежности:

- средняя наработка на отказ, ч;

- среднее время восстановления работоспособного состояния, ч;

- средний срок службы, лет.

При установлении показателей надежности должны быть указаны критерии отказа.

По требованию заказчика на конкретные средства и системы могут быть установлены дополнительно другие требования по надежности.

3.10.2. Средняя наработка на отказ ТС и подсистем (систем) ИСБ определяется действующими нормативными документами для каждой из подсистем (систем) и соответствующими техническими условиями для ТС.

3.10.3. Средний срок службы ТС и подсистем (систем) ИСБ определяется действующими нормативными документами для каждой из подсистем (систем) и соответствующими техническими условиями для ТС.

3.11. Требования к электропитанию.

3.11.1. Основное электропитание подсистем (систем) ИСБ должно осуществляться от сети переменного тока частотой 50±1 Гц с номинальным напряжением 220 В.

Подсистемы (систем) ИСБ должны быть работоспособны при допустимых отклонениях напряжения сети от минус 15 до +10 %.

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

3.11.2. Подсистемы (системы) ИСБ должны иметь резервное электропитание при пропадании напряжения основного источника питания. В качестве резервных источников питания может использоваться резервная сеть переменного тока или источники питания постоянного тока.

Номинальное напряжение резервных источников питания постоянного тока выбирается из ряда: 12, 24 В.

Переход на резервное питание должен происходить автоматически без нарушения установленных режимов работы и функционального состояния подсистем (систем) ИСБ.

Подсистемы (системы) ИСБ должны быть работоспособны при допустимых отклонениях напряжений резервных источников от минус 15 до + 10 % от номинального значения.

3.11.3. Резервные источники питания должны обеспечивать выполнение основных функций подсистем (систем) ИСБ при пропадании напряжений в сети на время, определяемое действующими нормативными документами для каждой из подсистем (систем).

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.

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

3.11.5. При использовании в качестве источника резервного питания аккумуляторных или сухих батарей, рекомендуется иметь индикацию разряда батареи ниже допустимого предела.

3.11.6. В ИСБ рекомендуется применять резервные источники питания, позволяющие осуществлять удаленный контроль (на ПЦН) их состояний и основные параметры электропитания.

3.11.7. Химические источники питания, встроенные в идентификаторы СКУД, беспроводные извещатели подсистем (систем) охранной и тревожной сигнализации, должны обеспечивать работоспособность в течение времени, не менее трех лет.

3.12. Требования безопасности.

3.12.1. ТС ИСБ должны удовлетворять общим требованиям безопасности по ГОСТ 12.2.007.0, ГОСТ Р МЭК 60065, ГОСТ 12.2.003.

3.12.2. Материалы, комплектующие изделия, используемые для изготовления ТС ИСБ, должны быть экологически безопасны.

3.12.3.ТС ИСБ должны удовлетворять общим требованиям пожарной безопасности по ГОСТ 12.1.004 и нормам пожарной безопасности.

3.12.4. Электрическое сопротивление изоляции ТС ИСБ между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должно быть не менее значений, указанных в таблице 3.1.

Таблица 3.1 Требуемые значения сопротивления изоляции

Климатические условия эксплуатации	***Сопротивление изоляции, МОм, не менее***
Нормальные	20,0
При наибольшем значении рабочей температуры	5,0
При наибольшем значении относительной влажности	1,0

3.12.5. Электрическая прочность изоляции ТС ИСБ между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должна соответствовать требованиям ГОСТ 12997.

3.12.6. Сопротивление изоляции и электрическая прочность ТС ИСБ, предназначенных для применения в жилых помещениях, должны удовлетворять требованиям ГОСТ Р МЭК 60065.

3.12.7. Конкретные значения сопротивления изоляции и электрическая прочность изоляции должны быть указаны в технических условиях и эксплуатационных документах.

3.12.8. ТС ИСБ, предназначенные для эксплуатации в зонах с взрывоопасной средой, должны соответствовать требованиям ГОСТ Р 51330.0 и других стандартов и нормативных документов, регламентирующих требования к изделиям, предназначенным для работы во взрывоопасных средах.

3.13. Иные требования.

3.13. Иные требования (кроме выше перечисленных), как то:

- требования к функциональным характеристикам конкретных ТС ИСБ;
- требования к устойчивости ТС ИСБ;
- требования устойчивости к внешним воздействующим факторам;
- требования к конструкции, приведены в действующей нормативной документации и должны быть отражены в технических условиях и эксплуатационной документации конкретных ТС в ИСБ.

4. ВЫБОР ИСБ ДЛЯ ОБОРУДОВАНИЯ ОБЪЕКТОВ

4.1. При выборе интегрированных систем безопасности, для оборудования ими 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 системы;

- 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.

4.2. При построении ИСБ объекта также необходимо руководствоваться рядом принципов, упрощающим установку всех элементов системы, их обслуживание, а также положительно сказывающимися на соотношении стоимость / качество.

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

4.2.2. 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.

4.2.3. 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".

4.2.4. 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.

4.3. 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.

4.4. 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 технических средств подсистем ИСБ.

4.5. По результатам обследования определяются тактико-технические характеристики и структура подсистем ИСБ и составляется техническое задание на оборудование объекта.

В техническом задании необходимо указать:

- назначение ИСБ, техническое обоснование и описание системы;
- размещение составных частей системы;
- условия эксплуатации ТС подсистем ИСБ;
- основные технические характеристики ТС подсистем ИСБ;

- требования к маскировке и защите ТС подсистем ИСБ от вандализма;

- оповещение 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 подсистем ИСБ в аварийных и чрезвычайных ситуациях;

- программное обеспечение системы;

- требования к безопасности;

- требования к электропитанию;

- обслуживание и ремонт подсистем ИСБ.

4.6. При наличии агрессивных условий эксплуатации: вне закрытых отапливаемых помещений, помещений с повышенным содержанием пыли, влажности воздуха, низкой температурой, следует ориентироваться на специализированные ТС подсистем ИСБ, предназначенные для работы в особых условиях. Надежность системы. Для надежной работы подсистем ИСБ на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, удаленность составных частей от управляющего центра, заземление ТС подсистем ИСБ и т.п.

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

- возможность максимальной синхронизации всех составляющих ИСБ устройств;

- 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 подсистем ИСБ во всех используемых режимах.

При требуемом уровне охраны объект, техническая, программная, информационная и эксплуатационная совместимость

элементов ИСБ характеризуется единством функций и технических характеристик, при:

- взаимодействии всех технических средств и устройств систем;

- 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.

5. ПРОЕКТИРОВАНИЕ ИСБ ОБЪЕКТА

5.1. Проектирование ИСБ включает следующие этапы работ:

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

- проведение обследования объекта и по результатам обследования составляется акт обследования;

- разработка и утверждение технического задания на разработку проектной документации (реконструкцию) ИСБ объекта;

- разработка проектной документации.

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

В состав комиссии обследования объектов, принимаемых под охрану подразделениями вневедомственной охраны МВД России, включаются представители подразделений вневедомственной охраны МВД России.

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

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

2) схема дорог по территории объекта и прилегающих к нему;

исходные данные для проектирования в составе:

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

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

5) отчеты по геологическим изысканиям;

6) анализ возможных криминальных угроз;

7) Классификация объекта по РД 78.36.003-2002;

8) какими средствами инженерной укрепленности и техническими средствами охраны оборудован объект;

9) указания по оборудованию средствами инженерной укрепленности и техническими средствами охраны, по разбитию на охранные и тревожные зоны, по определению рубежности охраны 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 акту.

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

Техническое задание на проектирование ИСБ разрабатывается заказчиком или организацией, уполномоченной на проведение данного вида работ в соответствии с действующим законодательством, и согласовывается с подразделением вневедомственной охраны.

К техническому заданию прилагается:

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

2) схема дорог для определения маршрутов движения наряда (пешего или автотранспортного) по территории объекта и прилегающих территорий;

3) 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;

исходные данные для проектирования в составе:

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

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

6) технические условия на подключение электронагрузок проектируемой системы;

7) отчеты по геологическим изысканиям; комиссия проектной документации

5.1.3. Проектная документация должна содержать следующий комплект документов:

1) техническое задание на разработку проекта;

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

3) рабочие чертежи, содержащие: структурные схемы, планы расположения оборудования, трассы прокладки кабелей, схемы подключения, требования к монтажу, кабельный журнал, схемы монтажа извещателей и приборов;

4) спецификации оборудования и материалов;

5) сметную документацию;

6) чертежи не стандартизованного оборудования или задания на его разработку;

7) эксплуатационная документация на ИСБ объекта;

8) эксплуатационная документация на технические средства, входящие в состав ИСБ объекта;

9) инструкция дежурного оператора ИСБ;

10) сертификаты на оборудование и используемые материалы.

5.1.4. Проектная документация согласовывается с 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 проектной документации.

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

6. ПРИМЕНЕНИЕ ИСБ НА ВЗРЫВООПАСНЫХ ОБЪЕКТАХ

6.1. 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.

6.2. Действующими нормативными документами в области взрывозащищенного оборудования являются ГОСТ Р 51330 "Электрооборудование взрывозащищенное", который соответствует требованиям международной электротехнической комиссии (МЭК) и европейским стандартам, 7 раздел Правил устройства электроустановок (ПУЭ).

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

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

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

I - рудничный метан;

II - остальные промышленные газы и пары.

ТС охраны ИСБ относятся к группе II - оборудованию для внутренней и наружной установки (кроме рудничного).

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

1) взрывонепроницаемая оболочка “d”;

2) искробезопасная электрическая цепь “i”.

6.4.1. 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 случаи должны быть выполнены с применением этого вида взрывозащиты, провода шлейфа сигнализации, интерфейсов и питания 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 технических средств ИСБ не ограничивается.

6.4.2. 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, мощный светозвуковой оповещатель.

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 требуют специального технического обслуживания, связанного с взрывозащитой.

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

6.5.1. В маркировку в указанной ниже последовательности входят:

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

2) знак Ex, указывающий на соответствие электрооборудования стандартам на взрывозащищенное электрооборудование. ("Ex", - от английского explosion - взрыв);

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

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

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

6.5.2. 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.

6.6. Уровень взрывозащиты - степень взрывозащиты электрооборудования при установленных нормативными документами условиях.

Установлены три уровня взрывозащиты электрооборудования:

1) Электрооборудование повышенной надежности против взрыва - взрывозащищенное электрооборудование, в котором взрывозащита обеспечивается только в признанном нормальном режиме его работы. Знак уровня - «2Ex».

2) 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».

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

6.7. Маркировка вида взрывозащиты.

6.7.1. Взрывонепроницаемая оболочка маркируется буквой «d».

6.7.2. Искробезопасная электрическая цепь маркируется буквой «i».

6.8. 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 6.1. Это подразделение базируется на безопасном экспериментальном максимальном зазоре (БЭМЗ) оболочек или минимальном токе воспламенения (МТВ) для электрооборудования с искробезопасными цепями.

Таблица 6.1. 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

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.

6.9. 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. 6.2.

Таблица 6.2. Температурные классы электрооборудования группы II

Знак температурного класса электрооборудования	*Предельная температура, °С*	*Группа взрывоопасной смеси, для которой электрооборудование является взрывозащищенным*
Т1	450	Т1
Т2	300	Т1, Т2
Т3	200	Т1-Т3
Т4	135	Т1-Т4
Т5	100	Т1-Т5
Т6	85	Т1-Т6

6.10. Для того чтобы установить, какой уровень взрывозащиты должны иметь ТС ИСБ необходимо определить класс взрывоопасной зоны. Согласно ПУЭ п.7.3.38, класс взрывоопасной зоны должен определяться технологами совместно с электриками проектной или эксплуатирующей организации.

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

6.10.2. 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.

6.11. Порядок монтаж электропроводок во взрывоопасных помещениях приведен в разделе 7 «Монтаж электропроводок объектовых технических средств ИСБ», порядок заземления или зануления во взрывоопасных зонах приведен в разделе 8 «Заземление ТС ИСБ» настоящих рекомендаций.

6.12. С видом взрывозащиты «взрывонепроницаемая оболочка» выпускается извещатель для работы в подсистеме СОС - ИО209-22 «СПЭК-11», уровень взрывозащиты «взрывобезопасный», маркировка взрывозащиты 1ExdIIBT5X

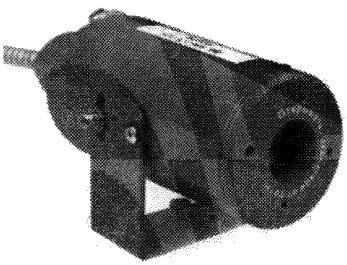


Рис. 6.1 Извещатель «СПЭК - 11»

Этот извещатель предназначен для применения в неагрессивных средах во взрывоопасных зонах помещений классов 1 или 2 по ГОСТ Р 51330.9 (классы В-Іа, В-Іб, В-Іг 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 ППК, обеспечивающим такие параметры в ШС.

Кронштейн для юстировки включен в комплект поставки извещателя.

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

Технические характеристики извещателя «СПЭК-11»

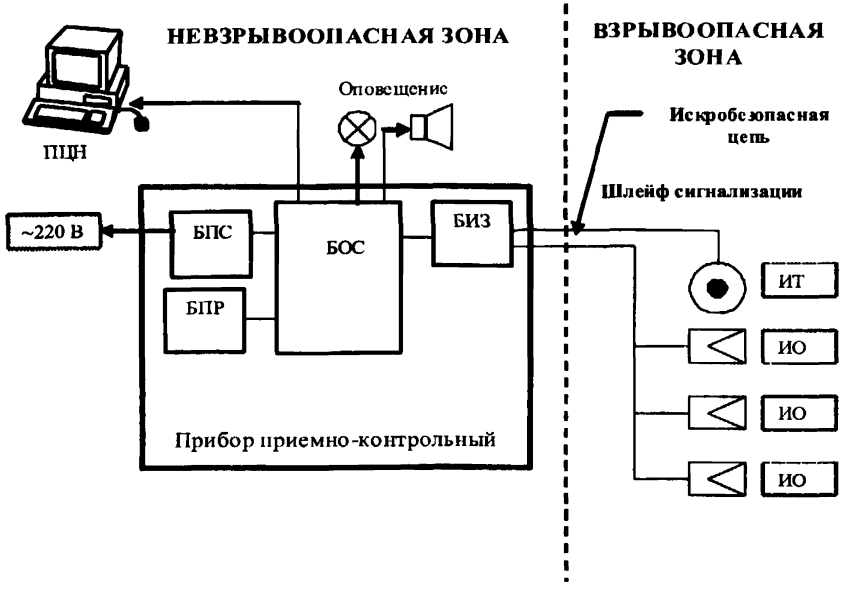
Дальность действия, м при коэффициенте запаса	125 25
Напряжение питания, В	от 10 до 27
Чувствительность, мс	130
Длительность извещения «Тревога», с, не менее	2
Диапазон рабочих температур, °С	От минус 40 до плюс 35
Габариты БИ, БФ, мм без учета кронштейна и кабеля в металлорукаве	155 х 95 х 85
Масса,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

6.13. 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 техническим средствам ИСБ. Но в этом случае технические средства 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

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

6.14.1 Пример оборудования объекта с взрывоопасными зонами приведен на рисунке 6.2



Условные обозначения:

ПЦН - пульт централизованного наблюдения;
БПС - блок питания сетевой;
БПР - блок питания резервный;
БОС - блок обработки сигналов;
БИЗ - блок искрозащиты;
ИТ - извещатель тревожный;
ИО - извещатель охранный.

Рис.6.2 Оборудование объекта с взрывоопасными зонами.

6.15. Примером подсистемы, предназначенной для организации охраны взрывоопасных зон помещений с неагрессивной средой является подсистема «Ладога-Ех» в составе ИСБ (прибора приемно-контрольного охранно-пожарного) «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 ШС «БРШС-Ех», обеспечивающий питание и прием извещений от извещателей, установленных во взрывоопасной зоне по искробезопасным шлейфам;
- извещатель оптико-электронный объемный ИО409-40 «Фотон-18»;
- извещатель оптико-электронный линейный ИО209-30 «Фотон-18А»;
- извещатель оптико-электронный поверхностный ИО309-18 «Фотон-18Б»;
- извещатель оптико-электронный поверхностный ИО309-21 «Фотон-Ш-Ех»;
- извещатель поверхностный звуковой ИО329-9 «Стекло-Ех»;
- извещатель поверхностный вибрационный ИО313-6 «Шорох-Ех»;
- извещатель точечный магнитоконтактный ИО102-33 «МК-Ех» исполнение 1;
- извещатель точечный магнитоконтактный ИО102-33 «МК-Ех» исполнение 2;
- сигнализатор тревожный газовый «СТГ-Ех»;
- сигнализатор тревожный затопления «СТЗ-Ех».

Блок расширения шлейфов сигнализации «БРШС-Ех».

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.

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

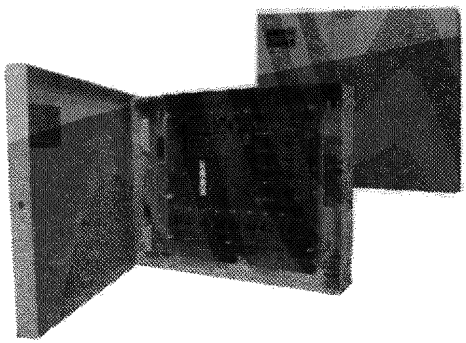


Рис. 6.3 Блок расширения шлейфов сигнализации.

Технические характеристики блока «БРШС-Ех»

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 питания - номинальное выходное напряжение, В - номинальный выходной ток, мА исп. 1	 12 200 625
Диапазон рабочих температур, °С	от плюс 1 до плюс 50
Габариты , мм	230 х 177 х 50
Масса, кг	1,5

Извещатели охранные оптико-электронные «Фотон-18»

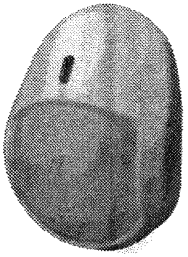


Рис.6.4 Извещатель «Фотон-18»

Предназначены для обнаружения проникновения в охраняемое пространство взрывоопасных зон закрытого помещения.

Особенности:

три зоны обнаружения формируются тремя типами линз Френеля:

-объемная - «Фотон-18»,

-линейная - «Фотон-18А»,

-поверхностная - «Фотон-18Б».

Технические характеристики извещателей «Фотон-18»

Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания	От 9 до 14 В
Ток потребления	Не более 20 мА
Дальность действия (зона обнаружения)	12 м (объемная) 20 м (линейная) 15 м (поверхностная)
Габаритные размеры	105x75x56 мм
Масса	Не более 0,1 кг
Степень защиты оболочки	IP41
Диапазон рабочих температур	-30…+50°С

Извещатель охранный поверхностный оптико-электронный «Фотон-Ш-Ех»

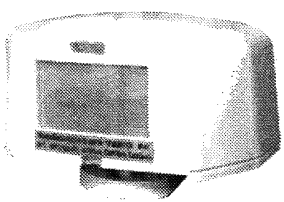


Рис.6.5 Извещатель «Фотон-Ш-Ех»

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.

Зона обнаружения аналогична зоне извещателя «Фотон-Ш».

Технические характеристики извещателя «Фотон-Ш-Ex»

Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания	От 9 до 14 В
Ток потребления	Не более 20 мА
Габаритные размеры	91x52x56 мм
Масса	не более 0,2 кг
Степень защиты оболочки	IP41
Диапазон рабочих температур	-30...+50°С

Извещатель поверхностный звуковой ИО329-9 «Стекло-Ex»

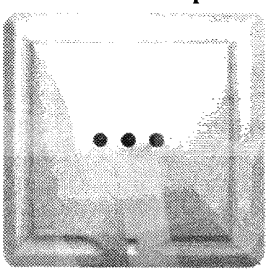


Рис.6.6 Извещатель «Стекло-Ex»

Предназначен для обнаружения разрушения обычного, закаленного, армированного, узорчатого, трехслойного (триплех), 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 «Стекло-Ех»

Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания, В	от 9 до 14
Ток потребления, мА	30
Максимальная дальность действия, м	6
Диапазон рабочих температур, °С	от минус 20 до плюс 45
Габариты , мм	80 х 80 х 35
Масса, кг не более	0,12

Извещатель поверхностный вибрационный ИО313-6 «Шорох-Ех»

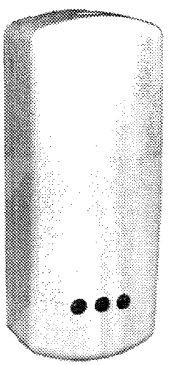


Рис 6.7 Извещатель «Шорох-Ех»

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 «Шорох-Ех»

Маркировка взрывозащиты	1ExibIIBT6X
Напряжение питания, В	от 9 до 14
Ток потребления, мА	20
Чувствительность к вибрации, с2	0,1 - 1,6
Диапазон рабочих температур, °С	от минус 30 до плюс 50
Габариты , мм	105 х 45 х 35
Масса, кг не более	0,3

Извещатель охранный точечный магнитоконтактный ИО102-33 «МК-Ех»

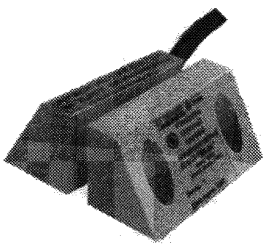


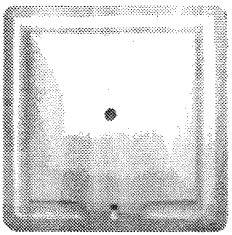
Рис 6.8 Извещатель «МК-Ех»

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 «МК-Ех»

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 х 45 х 35

Сигнализатор тревожный газовый «СТГ-Ех»



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

Рис 6.9 Сигнализатор «СТГ-Ех»

Технические характеристики сигнализатора «СТГ-Ех»

Маркировка взрывозащиты	[Exib]ВТ6Х
Напряжение питания, В	от 10 до 13
Ток потребления, мА	не более 50
Габаритные размеры, мм	80х80х35
Масса, кг не более	0,1
Степень защиты оболочки	IP30
Диапазон рабочих температур, °С	-30…+50

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 (БОС) и до трех датчиков затопления (ДЗ)

Технические характеристики сигнализатора «СТЗ-Ех»

Маркировка взрывозащиты	[Exib]ВТ6Х
Напряжение питания, В	От 9 до 14
Ток потребления, мА не более	10
Габаритные размеры, мм/масса, кг - БОС - датчик	 80х80х35 / 0,08 35х15х15 / 0,007
Степень защиты оболочки	IP40
Диапазон рабочих температур, °С	-30…+50

7. ВВОД В ЭКСПЛУАТАЦИЮ ИСБ

7.1. Приём ИСБ в эксплуатацию производится рабочей комиссией, в которую включаются представители:

1) заказчика;

2) службы охраны объекта;

3) монтажной и наладочной организации;

4) организации, производящей техническое обслуживание

4) подразделения вневедомственной охраны МВД России, осуществляющего охрану объекта;

5) при необходимости могут быть привлечены специалисты других организаций и ведомств.

7.2. При приемке выполненных работ по монтажу и наладке ИСБ рабочая комиссия осуществляет:

1) проверку качества выполненных монтажных и наладочных работ и их соответствие проектной документации;

2) 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 наладку, обязана устранить их в срок, установленный комиссией, и вновь предъявить смонтированную ИСБ к сдаче в эксплуатацию.

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

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

2) испытания работоспособности ИСБ дали положительные результаты.

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

Основные задачи технического обслуживания эксплуатации ИСБ:

1) обеспечение бесперебойного функционирования;

2) контроль технического состояния ИСБ и определение пригодности к дальнейшей эксплуатации;

3) выявление и устранение неисправностей и причин ложных срабатываний СОС, уменьшение их количества;

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

5) проведение ремонта.

8. ПЕРЕЧЕНЬ ОБЪЕКТОВ, ПОДЛЕЖАЩИХ ОБЯЗАТЕЛЬНОЙ ОХРАНЕ

8.1. Перечень объектов, подлежащих обязательной охране подразделениями вневедомственной охраны при органах внутренних дел Российской Федерации определен распоряжением Правительства Российской Федерации от 2 ноября 2009 г. № 1629-р.

8.2. Перечень объектов, подлежащих государственной охране определен Постановлением Правительства Российской Федерации от 2 ноября 2009 г. № 886.

8.3. Объекты противокриминальной охраны. В соответствии с ГОСТ Р 52551-2006 «Системы охраны и безопасности. Термины и определения» охраняемые объекты подразделяются на:

- **объект критически важный**: объект, нарушение или прекращение функционирования которого приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению, разрушению или существенному снижению безопасности жизнедеятельности населения, проживающего на этой территории, на длительный период времени;

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

- **объект повышенной опасности**: объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво- и пожароопасные, пожароопасные химические и биологические вещества, создающие реальную угрозу жизни и здоровью людей, а также окружающей среде.

9. СПИСОК ДЕЙСТВУЮЩИХ НОРМАТИВНЫХ ДОКУМЕНТОВ В ОБЛАСТИ ИСБ

9.1. ГОСТ 26342 - 84: Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры.

9.2. ГОСТ 27990 - 88: Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования.

9.3. ГОСТ 4.188 - 85: Система показателей качества продукции. Средства охранной, пожарной и охранно-пожарной сигнализации. Номенклатура показателей.

9.4. ГОСТ Р 50775-95 (МЭК 60839-1-1-1988): Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения.

9.5. ГОСТ Р 50776-95 (МЭК 60839-1-4-1989): Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по эксплуатированию, монтажу и техническому обслуживанию.

9.6. ГОСТ Р 50777-95/МЭК 60839-2-6-1990: Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 6. Пассивные оптико-электронные инфракрасные извещатели для закрытых помещений и открытых площадок.

9.7. ГОСТ Р 50659-94/МЭК 60839-2-5-1990: Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 5. Радиоволновые доплеровские извещатели.

9.8. ГОСТ Р 50658-94 (МЭК 60839-2-4-1990): Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений.

9.9. ГОСТ Р 52434-2005 (МЭК 60839-2-3-1987): Извещатели охранные оптико-электронные активные. Общие технические требования и методы испытаний.

9.10. ГОСТ Р 51186 - 1998 Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний.

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

9.12. ГОСТ Р 51242 - 98 Конструкции защитные механические и электромеханические для дверных и оконных проемов. Технические требования и методы испытаний на устойчивость к разрушающим воздействиям.

9.13. ГОСТ Р 51558 - 2008 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

9.14. ГОСТ Р 52435 - 2005 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.

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

9.16. ГОСТ Р 52551 - 2006 Системы охраны и безопасности. Термины и определения.

9.17. ГОСТ Р 52651 - 2006 Извещатели охранные комбинированные радиоволновые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний.

9.18 ГОСТ Р 52650 - 2006 Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний.

9.19. ГОСТ Р 52933 - 2008 Извещатели охранные поверхностные емкостные. Общие технические требования и методы испытаний.

9.20. ГОСТ Р 53702 - 2009 Извещатели охранные вибрационные пассивные для блокировки строительных конструкций закрытых помещений и сейфов. Общие технические требования и методы испытаний.

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

9.22. ГОСТ Р 54126 - 2010 Оповещатели охранные. Классификация. Общие технические требования и методы испытаний.

10. СПИСОК РЕКОМЕНДАЦИЙ, РУКОВОДЯЩИХ ДОКУМЕНТОВ И МЕТОДИЧЕСКИХ ПОСОБИЙ В ОБЛАСТИ ИСБ

10.1. Технические средства систем безопасности объектов. Обозначения условные и графические элементов систем (РД 78.36.002 - 2010).

10.2. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств (РД 78.36.003 - 2002).

10.3. Рекомендации о техническом надзоре за выполнением проектных, монтажных и пусконаладочных работ по оборудованию объектов техническими средствами охраны (РД 78.36.004 - 2005).

10.4. Рекомендации о порядке обследования объектов, принимаемых под охрану (РД 78.36.005 - 2005).

10.5. Рекомендации по выбору и применению технических средств охранно-пожарной сигнализации и средств инженерно-технической укрепленности для оборудования объектов (РД 78.36.006 - 2005).

10.5. Выбор и применение телевизионных систем видеоконтроля: Рекомендации (Р 78.36.002 - 2010).

10.7. Выбор и применение систем контроля и управления доступом. Рекомендации (Р 78.36.005-2010).

10.8. Инженерно - техническая защита нетелефонизированных объектов. Рекомендации (Р 78.36.010 - 2000).

10.9. Ложные срабатывания технических средств охранной сигнализации и методы борьбы с ними (Р 78.36.013 - 2002).

10.10. Методическое пособие «Системы охранного телевидения» (2008г.)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ **3**

1 ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ **5**

2 ПРИНЦИПЫ ИНТЕГРАЦИИ И КЛАССИФИКАЦИЯ ИСБ **9**

3 ТРЕБОВАНИЯ К ИСБ **18**

3.1 Общие положения 18

3.2 Требования к аппаратным средствам и программному обеспечению ИСБ 20

3.3 Технические и организационные меры по защите информации ИСБ 21

3.4 Требования к системе охранной и тревожной сигнализации 23

3.5 Требования к системе контроля и управления доступом 27

3.6 Требования к системе охранной телевизионной 32

3.7 Требования к подсистемам оповещения 39

3.8 Требования к подсистеме защиты от краж отдельных предметов 40

3.9 Требования к электромагнитной совместимости 41

3.10 Требования к надежности 41

3.11 Требования к электропитанию 42

3.12 Требования безопасности 44

3.13 Иные требования 45

4 ВЫБОР ИСБ ДЛЯ ОБОРУДОВАНИЯ ОБЪЕКТОВ **45**

5 ПРОЕКТИРОВАНИЕ ИСБ ОБЪЕКТА **49**

6 ПРИМЕНЕНИЕ ИСБ НА ВЗЫВООПАСНЫХ ОБЪЕКТАХ **52**

7 ВВОД В ЭКСПЛУАТАЦИЮ ИСБ **67**

8 ПЕРЕЧЕНЬ ОБЪЕКТОВ, ПОДЛЕЖАЩИХ ОБЯЗАТЕЛЬНОЙ ОХРАНЕ **68**

9 СПИСОК ДЕЙСТВУЮЩИХ НОРМАТИВНЫХ ДОКУМЕНТОВ В ОБЛАСТИ ИСБ **69**

10 СПИСОК РЕКОМЕНДАЦИЙ, РУКОВОДЯЩИХ ДОКУМЕНТОВ И МЕТОДИЧЕСКИХ ПОСОБИЙ В ОБЛАСТИ ИСБ **71**

gost.e-ecolog.ru