

**МЕТОДИЧЕСКИЕ      РАЗРАБОТКИ**

для проведения занятий

по учебной дисциплине:

***«Техническая подготовка»***

по теме:

***Технические средства охраны объектов***

«УТВЕРЖДАЮ»

Директор НОЧУ ДПО «Варяг»

\_\_\_\_\_ В.Н. Матвеев  
«\_\_» \_\_\_\_\_ 201\_\_ года

## МЕТОДИЧЕСКАЯ РАЗРАБОТКА

по «Технической подготовке»

профессиональной подготовки частных охранников 4 разряда (5, 6)

Тема № 1 Технические средства охраны объектов.

Время: 6 часов

**Цель занятия:** 1. Усвоение обучаемыми доведённых во время занятия требований нормативных документов, регламентирующих требования по инженерно-технической укреплённости и защите объектов.

2. Ознакомления слушателей с основными видами конструктивных и технических средств обеспечивающих противодействие несанкционированному проникновению, взлому и другим преступным посягательствам.

**Вопросы:**1. Основные термины и определения применяющиеся в охранной деятельности. Назначение и классификация охраняемых объектов. Инженерно-техническая укреплённость охраняемых объектов.

2. Технические средства охранной и тревожной сигнализации. Защита периметра территории и открытых площадок. Защита здания, помещений, отдельных предметов. Защита персонала и посетителей объекта. Организация передачи информации о срабатывании сигнализации.

3. Системы контроля и управления доступом. Системы охранного телевидения. Системы оповещения. Системы охранного освещения. Электроснабжение технических средств охраны.

4. Виды технических средств и систем охранной, охранно-пожарной сигнализации. Назначение и принцип действия охранных датчиков (извещателей). Назначение и принцип действия пожарных датчиков (извещателей). Охранные извещатели и оповещатели.

5. Технические средства сбора и обработки информации

## **ВОПРОС № 1. НАЗНАЧЕНИЕ И КЛАССИФИКАЦИЯ ОХРАНЯЕМЫХ ОБЪЕКТОВ.**

Основные термины и определения встречающиеся в системе охраны различных объектов:

**Инженерно-техническая укрепленность объекта:** совокупность прочностных характеристик и свойств конструктивных элементов зданий, помещений и охраняемых территорий, обеспечивающих необходимое противодействие несанкционированному проникновению в охраняемую зону, взлому и другим преступным посягательствам.

**Криминальная угроза** – совокупность условий и факторов, создающих опасность преднамеренного противоправного вторжения или нанесения ущерба объекту или находящимся на нем людям.

**Категория охраняемого объекта:** комплексная оценка объекта, учитывающая его экономическую или иную (например, культурную) значимость, в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных преступных посягательствах на них, сложности обеспечения требуемой охраны.

**Ловушка (при охране):** охранный датчик (извещатель), скрытно устанавливаемый:

- внутри охраняемого объекта на наиболее вероятном направлении перемещения нарушителя, блокирующий участок, зону, объем;
- для блокировки отдельного предмета, либо препятствующего намерениям нарушителя (например, стоящий перед дверью сейфа стул), либо могущего стать целью преступного посягательства (например, какого-либо имущества);
- для блокировки мест возможного проникновения из подвальных, чердачных и других смежных неохраняемых помещений.

**Нарушитель:** лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищённое системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, охранника, пользователя или жильца.

**Особо важный объект:** объект, значимость которого определяется органами государственной власти Российской Федерации или местного самоуправления, с целью определения мер по защите интересов государства, юридических и физических лиц от преступных посягательств и предотвращения ущерба, который может быть нанесён природе и обществу, а также от возникновения чрезвычайной ситуации (Администрация области и города, органы УВД, ФСБ, суда и судебный департамент, гостиницы, больницы и т.п., «Акрон»)

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

**Объект повышенной опасности или потенциально опасный объект:** объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво-, пожароопасные, опасные химические и биологические вещества, создающие реальную угрозу возникновения источника чрезвычайной ситуации («Акрон», БОС - большие очистные сооружения, мясокомбинат, молокозавод, рыбоконсервный комбинат, новгородский хлеб и другие).

**Объект критически важный** – объект, нарушение и прекращение функционирования

которого приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, её необратимому негативному изменению, разрушению или существенному снижению безопасности жизнедеятельности населения, проживающего на этой территории, на длительный период времени (БОС - большие очистные сооружения и водозаборные станции; электро и газоподающие, нефтеперелеевые станции).

**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 (Атомные электростанции, захоронения атомных и биологических веществ).

**Объект с массовым пребыванием граждан** – здание или сооружение с одновременным пребыванием 50 и более человек (зрительные, обеденные, выставочные, торговые, биржевые, спортивные, культовые и другие залы).

**Охраняемый объект:** предприятие, организация, офисы, строящиеся объекты, жилище, промышленные и продуктовые объекты, оборудованные действующей системой охраны и безопасности.

**Пульт централизованного наблюдения (ПЦН):** техническое средство (совокупность технических средств) или составная часть системы передачи извещений, устанавливаемая в пункте централизованной охраны для приёма от пультовых оконечных устройств или ретрансляторов извещений о проникновении, разбойном нападении на охраняемые объекты и/или пожаре на них.

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

**Рубеж охранной сигнализации:** шлейф или совокупность шлейфов сигнализации, контролируемых охраняемые зоны территории, здания или помещения (1 рубеж – периметр, территория, 2 рубеж - объем или площадь охраняемого объекта, 3 рубеж - сами ценности или подходы к ним) на пути возможного движения нарушителя к материальным ценностям, при преодолении которых выдаётся соответствующее извещение о проникновении.

**Шлейф сигнализации:** цепь (электрическая, радиоканальная, оптоволоконная или другая) соединяющая выходные узлы извещателей, включающая в себя вспомогательные (выносные) элементы и соединительные линии и предназначенная для передачи на прибор приёмно-контрольный (ППК) или на устройство объективное системы передачи извещений (СПИ) информации от извещателей о контролируемых ими параметрах, а в некоторых случаях - для подачи электропитания на извещатели.

**Зона** - это часть охраняемого объекта, контролируемая одним или несколькими шлейфами сигнализации. Поэтому термин "зона", используемый в описаниях зарубежной аппаратуры, является в данном случае синонимом термина "шлейф сигнализации".

**Зона обнаружения извещателя** - часть пространства охраняемого объекта, в которой извещатель выдаёт тревожное извещение при превышении контролируемым параметром порогового значения данного извещателя.

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

**Система охранной сигнализации:** совокупность совместно действующих технических средств обнаружения проникновения (попытки проникновения) на охраняемый объект, сбора, обработки, передачи и представления в заданном виде информации о проникновении (попытки проникновения) и другой служебной информации.

**Система тревожной сигнализации:** совокупность совместно действующих технических средств, позволяющих автоматически или в ручную выдавать сигналы тревоги на ПЦО (в службы охраны или в группу быстрого реагирования) при разбойном нападении на объект в период его работы.

**Техническое средство охраны:** конструктивно законченное, выполняющее самостоятельные функции устройство, входящее в состав систем охранной, тревожной сигнализации, контроля и управления доступом, охранного телевидения, освещения, оповещения и других систем, предназначенных для охраны объекта.

**Типовые проектные решения:** технические решения оборудования техническими средствами охраны и элементами инженерно-технической укрепленности ряда аналогичных по назначению и конструктивно-строительным характеристикам объектов или их отдельных конструкций.

**Устойчивость к взлому** – способность конструкции противостоять разрушающему воздействию приводящему к утрате конструкцией заданных целевых физических свойств и функций назначения.

**Ущерб от преступного посягательства:** экономические, экологические или социальные последствия (убытки, потери) от преступного посягательства на охраняемый объект.

**Усиление инженерно-технической укрепленности объекта** – совокупность мероприятий направленных на усиление конструктивных элементов зданий, помещений и территорий, оснащение объекта дополнительными средствами инженерно-технической укрепленности соответствующего класса защиты, для обеспечения соответствия требованиям, предъявляемым к установленной категории объектов.

**Оптическая плотность среды** - десятичный логарифм отношения потока излучения, прошедшего через незадымленную среду, к потоку излучения, ослабленного средой при ее частичном или полном задымлении.

**Режим охраны** — это сочетание действий службы охраны, инженерно-технических средств и режимных мероприятий, направленных на обеспечение полной, частичной (выборочной), сохранности материальных ценностей, персонала охраняемого объекта, а также интеллектуальной собственности и ценной информации о деятельности этого объекта. В значительной степени режим охраны объекта характеризует круг обязанностей и меры ответственности охраны.

**К основным задачам режима охраны относятся: обеспечение сохранности зданий и помещений; сохранность и контроль за перемещением материальных ценностей; обеспечение пропускного режима или, если он не предусмотрен, контроль за допуском граждан в здания и помещения; обеспечение безопасности сотрудников и руководства, а также объекта в ночное время; поддержание противопожарной безопасности (если этими вопросами не занимаются специальные службы и лица)**

## **Назначение и классификация охраняемых объектов по категориям.**

В зависимости от значимости и концентрации материальных, художественных, исторических, культурных и культовых ценностей, размещенных на объекте, последствий от возможных преступных посягательств на них, все объекты, их помещения и территории подразделяются на две группы (категории): А и Б. Ввиду большого разнообразия разнородных объектов в каждой группе, они дополнительно подразделяются на две подгруппы каждая: АI и АII, БI и БII.

Для оценки возможных последствий реализации криминальных угроз используют виды ущерба:

- государственно-политический ущерб – ухудшение криминогенной обстановки в стране (регионе), негативный международный и общественный резонанс, негативные публикации в СМИ, подрывающие международный авторитет государства, формирующие негативное отношение к органам внутренних дел;
- финансово-экономический ущерб, который определяется ст. 158 УК РФ<sup>3</sup> как:
- ущерб особо крупный – ущерб свыше 1 миллиона рублей;
- ущерб крупный – свыше 250 тысяч рублей;
- ущерб значительный – менее 250 тысяч рублей.

Для каждого класса объектов выбирается своя степень защиты от взлома, проникновения. 1-я степень (минимально необходимая); 2-я степень (средняя); 3-я степень (высокая); 4-я степень (очень высокая)

Объекты категорий А1, А2, и А3 (А1 категория - наивысшая) – это объекты Государственной Власти, критически важные объекты, особо важные объекты, потенциально опасные объекты и объекты жизнеобеспечения, государственные, а также коммерческие объекты, преступные посягательства на которые могут привести к особо крупному экономическому ущербу государству или собственнику имущества и иметь широкий международный и общественный резонанс;

Объекты категорий Б1 и Б2 – это объекты организаций различных форм собственности, преступные посягательства на которые могут привести к крупному и значительному материальному ущербу предприятию или собственнику.

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

### **Объекты подгруппы АI**

1. - Специальные помещения, расположенные на территории (в зданиях, сооружениях) объектов критически важных, особо важных и потенциально опасных объектов инфраструктуры Российской Федерации, объектов подлежащих обязательной охране полицией, определенных перечнями, утвержденными Правительством Российской Федерации:

- хранилища и кладовые (сейфовые комнаты) денежных и валютных средств, ценных бумаг;

- хранилища (сейфовые комнаты), ювелирных изделий, драгоценных металлов и камней;

- помещения с оборотом сведений, составляющих государственную тайну;

- хранилища (склады) огнестрельного оружия, взрывчатых веществ, сильнодействующих, ядовитых, бактериологических, токсичных веществ;

- хранилища наркотических и психотропных веществ и препаратов;

- хранилища федеральных государственных музеев, государственных архивов и федеральных библиотек.

## **Объекты подгруппы А2**

1. Государственные и коммерческие объекты с оборотом денежных средств, драгметаллов, драгоценных камней, ювелирных изделий и иных материальных и культурных ценностей, преступные посягательства на которые могут привести к особо крупному экономическому ущербу государству или собственнику имущества (не вошедшие в категорию А1):

- обособленные помещения (здания) критически важных объектов, особо важных и потенциально опасных объектов инфраструктуры Российской Федерации, объектов, подлежащих обязательной охране полицией в соответствии с перечнями, утвержденными Правительством Российской Федерации;

2. - объекты кредитно-финансовой системы (банки, операционные кассы, дополнительные офисы, кассы самообслуживания, банкоматы):

- объекты (комнаты) хранения оружия и боеприпасов, наркотических, сильнодействующих и психотропных веществ и препаратов, драгоценных металлов, камней и изделий из них;

3. - ювелирные магазины, базы, склады, и другие объекты, использующие в своей деятельности ювелирные изделия, драгоценные металлы и камни;

- помещения для хранения наличных денежных средств (хранилища, кассы) коммерческих банков, предприятий, организаций и учреждений;

- объекты (помещения) с обработкой сведений, составляющих персональные данные граждан;

- объекты с хранением и экспонированием предметов старины, искусства и культуры;

- помещения с хранением документов строгой отчетности или спецпродукции;

- объекты отправления религиозного культа, представляющие историческую ценность.

## **Объекты категории А3**

Критически важные и потенциально опасные объекты, объекты, подлежащие обязательной охране полицией, в соответствии с соответствующими перечнями, утверждаемыми Правительством Российской Федерации, особо важные объекты, объекты жизнеобеспечения, а также объекты с массовым пребыванием граждан, на которых охрана общественного порядка и материальных ценностей обеспечивается постами физической охраны и выводом тревожной сигнализации на ПЦО подразделений вневедомственной охраны:

- контрольно-пропускные пункты охраны (службы безопасности) объекта;
- служебные помещения и посты охраны (службы безопасности) объекта;
- иные служебные помещения внутри объекта;
- объекты образования, здравоохранения, культуры и спорта.

Объекты подгрупп БI и БII - это объекты, хищения на которых в соответствии с уголовным законодательством Российской Федерации могут привести к ущербу в

размере до 500 минимальных размеров оплаты труда и свыше 500 соответственно.

**Объекты подгруппы Б1:**

1. Объекты организаций различных форм собственности с сосредоточением материальных ценностей, преступные посягательства на которые могут привести к крупному или значительному ущербу собственнику имущества:

2. - объекты с хранением, размещением и реализацией товаров, предметов повседневного спроса, продуктов питания, табачной и алкогольной продукции;

- объекты организаций различных форм собственности (в том числе расположенные в жилых домах и в квартирах, выведенных из жилого фонда);

3. - объекты мелкооптовой и розничной торговли;

- иные объекты потребительского рынка;

- объекты ЖКХ (ТСЖ, управляющие компании).

**Объекты подгруппы Б2:**

1. Государственные или коммерческие объекты, собственниками которых принято решение об установке системы тревожной сигнализации:

2. - служебные помещения охраны ГСК, автостоянок, помещения консьержей в подъездах жилых домов;

3. - объекты капитального строительства (строительные площадки);

- объекты, подходящие по своему функциональному назначению и наличию материальных ценностей под категории Б1, администрация которых направила заявку на оборудование объекта только системой тревожной сигнализации.



## **Инженерно-техническая укрепленность охраняемых объектов.**

Средства инженерно-технической укрепленности объекта предназначены для защиты объекта и находящихся на нем людей путем создания физической преграды несанкционированным действиям нарушителя в отношении объекта и его персонала. Средства инженерно-технической укрепленности должны удовлетворять следующим требованиям:

- обладать прочностью и долговечностью;
- затруднять нарушителю несанкционированный проход через рубеж доступа;
- ограничивать использование нарушителем подручных средств;
- обеспечивать достаточную пропускную способность при санкционированном или аварийном доступе;
- не оказывать влияния на работу технических средств охраны;
- способствовать выполнению сотрудниками службы обеспечения безопасности объекта своих обязанностей.

К средствам инженерно-технической укрепленности относятся:

### **1. Ограждения периметра, отдельных участков территории**

Ограждения представляют собой инженерно-технические сооружения, препятствующие умышленному или непреднамеренному доступу людей на территорию охраняемого объекта.

***Б 325. Ограждение периметра (отдельных участков территории) охраняемого объекта, в соответствии с техническими нормами подразделяется на основное, дополнительное (расположенное сверху и снизу) и предупредительное (расположенное с внешней или с внутренней стороны от основного).***

**Основное ограждение должно исключать случайный проход людей (животных), въезд транспорта или затруднять проникновение нарушителей на охраняемую территорию, минуя контрольно-пропускной пункт (КПП).**

Ограждение должно выполняться в виде прямолинейных участков, с минимальным количеством изгибов и поворотов, ограничивающих наблюдение и затрудняющих применение технических средств охраны.

К ограждению не должны примыкать какие-либо пристройки, кроме зданий, являющихся продолжением периметра. Окна первых этажей этих зданий, выходящих на неохраемую территорию, должны оборудоваться металлическими решётками, а при необходимости - и металлическими сетками.

**Ограждение не должно иметь лазов, проломов и других повреждений, а также незапираемых дверей, ворот и калиток.**

Выбор конструкций и материалов основного ограждения объекта, обеспечивающих требуемую надёжность защиты объекта, производится в соответствии с классификацией объекта.

**Дополнительное ограждение устраивают для уменьшения уязвимости основного ограждения. Верхнее дополнительное ограждение устанавливается на основное ограждение, если высота последнего не менее 2,5 м. Оно может представлять собой козырёк, выполненный из 3 - 4 рядов колючей проволоки, инженерное средство защиты типа "Спираль АКЛ" или иное устройство. Нижнее дополнительное ограждение - для защиты от подкопа должно устанавливаться под основным ограждением с заглублением в грунт не менее 50 см. Оно должно выполняться в виде бетонированного цоколя или сварной решётки из прутков арматурной стали, диаметром не менее 16 мм, с ячейками размерами не более 150**

х 150 мм, сваренной в перекрестиях.

На крышах одноэтажных зданий, примыкающих к ограждению, следует также устанавливать дополнительное ограждение.

**Предупредительное ограждение, как правило следует устанавливать на особо важных объектах подгруппы А1. Оно может располагаться как с внешней, так и/или с внутренней стороны основного ограждения. Высота предупредительного ограждения должна быть не менее 1,5 м. На предупредительном ограждении должны размещаться таблички типа: “Не подходить! Запретная зона” и другие.**

Предупредительное ограждение должно быть просматриваемым и выполняться из штакетника, металлической сетки, гладкой или колючей проволоки или другого материала.

Для удобства обслуживания технических средств охраны, связи, оповещения и освещения, осмотра местности предупредительное внутреннее ограждение следует разбивать на отдельные участки. На каждом участке должна быть предусмотрена калитка.

При невозможности оборудования уязвимых мест ограждения техническими средствами охраны, необходимо размещать в этих местах посты охраны (постовые “грибки”) или проводить другие инженерно-технические и организационные мероприятия по усилению охраны.

**Б 327. В структуре ограждения периметра охраняемого частной охраной объекта могут применяться (использоваться): зона отторжения (участок между основным и внутренним предупредительным ограждением), контрольно-следовая полоса. При необходимости (оговаривается в техническом задании, акте обследования) вдоль основного ограждения периметра между основным и внутренним предупредительным ограждениями устраивается зона отторжения, контрольно-следовая полоса.**

В зоне отторжения размещаются:

- средства охранной сигнализации;
- охранное освещение, охранное телевидение;
- посты охраны (постовые “грибки”);
- средства связи постов и нарядов охраны;
- указательные и предупредительные знаки.

Зона отторжения должна быть тщательно спланирована и расчищена. В ней не должно быть никаких строений и предметов, затрудняющих применение технических средств охраны и действия службы безопасности. Зона отторжения может быть использована для организации охраны объекта с помощью служебных собак. В этом случае зона отторжения должна иметь предупредительное сетчатое или штакетное ограждение высотой не менее 2,5 м. Ширина зоны отторжения, в которой размещаются технические средства охраны периметра, должна превышать ширину их зоны обнаружения.

## **2. Ворота, калитки**

Ворота устанавливаются на автомобильных и железнодорожных въездах на территорию объекта. По периметру территории охраняемого объекта могут устанавливаться как основные, так и запасные или аварийные ворота. Ворота могут иметь самую различную конструкцию — откаточные или распашные,

решётчатые или сплошные, открываемые вручную или с помощью механического привода, полностью автоматические.

Конструкция ворот должна обеспечивать их жёсткую фиксацию в закрытом положении.

**Б 311. Технические требования к воротам с электроприводом и дистанционным управлением предусматривает оборудование ворот устройствами аварийной остановки и открытия вручную на случай неисправности или отключения электропитания.**

Ворота следует оборудовать ограничителями или стопорами для предотвращения произвольного открывания или закрывания (движения).

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

При использовании замков в качестве запирающих устройств основных ворот, следует устанавливать замки гаражного типа или висячие (навесные). Редко открываемые ворота (запасные или аварийные) со стороны охраняемой территории должны запираяться на засовы и висячие (навесные) замки.

Калитку следует запирасть на врезной, накладной замок или на засов с висячим замком. Усиление защиты калиток рекомендуется выполнять аналогично способам усиления дверей и их коробок .

На отдельных участках территории и с внешней стороны ворот на объектах подгруппы А1 следует устанавливать специальные устройства для ограничения скорости движения автотранспорта, а на особо важных объектах - противоударные устройства или использовать шлюзовую систему ворот.

Выбор конструкций и материалов ворот, обеспечивающих требуемую надёжность защиты объекта, производится в соответствии с классификацией объекта.

### **3. Контрольно-пропускной пункт**

Объект, на котором установлен пропускной режим или планируется его введение, должен оборудоваться КПП для прохода людей и проезда транспорта. КПП должен обеспечивать необходимую пропускную способность прохода людей и проезда транспорта.

В зависимости от категории объекта на КПП рекомендуется предусмотреть:  
помещение для хранения и оформления пропусков (карточек);  
камеру хранения личных вещей персонала и посетителей объекта;  
комнату досмотра;  
помещение для сотрудников охраны и размещения технических средств охраны.

Устройства управления механизмами открывания, прохода/проезда, охранним освещением и стационарными средствами досмотра должны размещаться в помещении КПП или на его наружной стене со стороны охраняемой территории. В последнем случае должен исключаться доступ к устройствам управления посторонних лиц.

Для осмотра автотранспорта на КПП должны быть оборудованы смотровые площадки, эстакады, а для осмотра железнодорожного транспорта - вышки с площадками.

Окна КПП и двери должны оборудоваться защитными конструкциями, соответствующего класса защиты. Для контроля подъезжающего транспорта и прибывающих граждан сплошные ворота и входная дверь на территорию объекта

должны быть оборудованы смотровыми окошками или “глазками”. Вход в КПП должен быть предусмотрен со стороны охраняемой территории. Для прохода людей через КПП необходимо предусмотреть коридор, оборудованный турникетами.

**Шлюз** — конструкция, состоящая из двух взаимосвязанных дверей или ворот, которая обеспечивает отдельный проход людей или проезд транспорта. Дверь или ворота на выход должны открываться только после блокирования входной двери или ворот шлюза.

**Турникет** — наиболее распространённое устройство, регулирующее проход людей, который может быть поясным (высота до 1,5 метров) и в полный рост человека. Наиболее распространёнными типами поясных турникетов являются: вращающиеся; сдвижные; распашные (калитка).

#### **4. Водопропуски, воздушные трубопроводы, подземные коллекторы**

Водопропуски сточных или проточных вод, подземные коллекторы (кабельные, канализационные) при диаметре труб или коллектора от 300 до 500 мм, выходящие с территории объектов подгруппы А1 должны оборудоваться на выходе с охраняемого объекта металлическими решётками. Решётки должны изготавливаться из прутков арматурной стали диаметром не менее 16 мм, образующих ячейки размером не более чем 150 x 150 мм, сваренных в перекрестиях. В трубах или коллекторах большего диаметра, где есть возможность применения инструмента взлома, необходимо устанавливать решетки, заблокированные охранной сигнализацией на разрушение или открывание.

Воздушные трубопроводы, пересекающие ограждения периметра, должны оборудоваться элементами дополнительного ограждения: козырьком из колючей проволоки или инженерным средством защиты типа “Спираль АКЛ”. Инженерное средство защиты “Спираль АКЛ” разворачивается по верху трубопровода или вокруг него.

## 5. Стены, перекрытия, перегородки зданий и помещений

Наружные и внутренние стены зданий, перекрытия пола и потолка помещений объектов должны быть труднопреодолимым препятствием для проникновения нарушителей и иметь соответствующий класс защиты от взлома, который достигается правильным выбором строительных материалов для их изготовления.

Для труднопреодолимого препятствия при проникновении - производят усиление стен, перекрытий и перегородок металлическими решётками (сетками) должно производиться по всей площади, устанавливаемыми с внутренней стороны помещения. Решётки (сетки) привариваются к прочно заделанным в стену на глубину 80 мм стальным анкерам диаметром не менее 12 мм (к закладным деталям из стальной полосы 100 x 50 x 6 мм, пристреливаемым четырьмя дюбелями), с шагом не более 500 x 500 мм. После установки решётки (сетки) должны быть замаскированы штукатуркой или облицовочными панелями.

Допускается, по согласованию с подразделением вневедомственной охраны, МЧС и ЧОП, установка решётки (сетки) с наружной стороны помещения.

## 6. Дверные конструкции

Двери объектов и их помещений, люки (далее - дверные конструкции) должны быть исправными, хорошо подогнанными под дверную коробку. Дверные конструкции должны обеспечивать надёжную защиту помещений объекта и обладать достаточным классом защиты к разрушающим воздействиям.

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

При применении сертифицированных дверей количество и класс замков указывается в соответствующей документации на дверь. При невозможности установки дополнительных дверей необходимо входные двери блокировать техническими средствами раннего обнаружения, выдающими тревожное извещение при попытке подбора ключей или взлома замка (замки типа «Супер Класс» со встроенным в ригель замка магнитоконтактным извещателем скрытой установки).

Двустворчатые двери должны оборудоваться двумя стопорными задвижками (шпингалетами), устанавливаемыми в верхней и нижней части одного дверного полотна. Сечение задвижки должно быть не менее 100 мм, глубина отверстия для неё - не менее 30 мм.

Для объектов подгруппы А I устанавливаются тамбуры безопасности (шлюзы).

***Б 306. В основу работы тамбура безопасности (шлюза), оборудуемого при входе (въезде) на охраняемый объект закладывается принцип поочерёдной блокировки дверей (ворот) — одна дверь (ворота) не открываются, пока не будет закрыта другая дверь (ворота).***

Дверные проёмы (тамбуры) центрального и запасных входов на объект, при отсутствии около них постов охраны, следует оборудовать дополнительной запирающейся дверью. Дополнительная дверь объектов подгрупп Б I и Б II должны быть не ниже 1-го класса защиты, а для объектов подгруппы А I - не ниже 2-го. Классы защиты основной входной двери и дополнительной допускается менять местами.

***Б 307. Допускается одновременное открытие обеих дверей (ворот) тамбура безопасности (шлюза) в случае режима экстренной эвакуации при какой либо чрезвычайной ситуации (пожар, наводнение, возможность взрыва и т. п.).***

При невозможности установки дополнительных дверей необходимо входные

двери блокировать техническими средствами охраны раннего обнаружения, выдающие тревожное извещение при попытке подбора ключей или взлома двери.

Дверные проёмы входов в специальные помещения объектов подгрупп АI и БII, в которых хранятся ценности (объекты подгруппы АII, сейфовые и оружейные, комнаты, кассы предприятия и другие аналогичные помещения, требующие повышенных мер защиты) должны быть оборудованы дополнительной запирающейся металлической решетчатой дверью. Дополнительная дверь обеспечивает как защиту от скоротечной кражи, так и защиту персонала в помещении при работе с открытой входной дверью.

## **7. Оконные конструкции**

Оконные конструкции (окна, форточки, фрамуги) во всех помещениях охраняемого объекта должны быть остеклены, иметь надёжные и исправные запирающие устройства. Стекла должны быть жёстко закреплены в пазах.

Оконные конструкции должны обеспечивать надёжную защиту помещений объекта и обладать достаточным классом защиты к разрушающим воздействиям.

Оконные проёмы касс предприятий, сейфовых и оружейных комнат, других специальных помещений, требующих повышенных мер защиты, независимо от этажности, в обязательном порядке должны быть оборудованы защитными конструкциями или защитным остеклением.

При оборудовании оконных конструкций металлическими решётками, их следует устанавливать с внутренней стороны помещения или между рамами. В отдельных случаях допускается, по согласованию с подразделением МЧС и вневедомственной охраны, установка решёток с наружной стороны при их обязательной защите техническими средствами охраны.

Если все оконные проёмы помещения оборудуются решётками, одна из них делается открывающейся (распашной, раздвижной). Решётка должна запирается с внутренней стороны помещения на замок соответствующего класса защиты или на иное устройство, обеспечивающее надёжное запирание решётки и эвакуацию людей из помещения в экстремальных ситуациях. Для больших помещений с количеством окон более 5, количество открывающихся решёток определяется условиями быстрой эвакуации людей.

Оконные проёмы первых этажей объектов с длительным (сезонным) отсутствием сотрудников или работников следует защищать щитами, ставнями не ниже 2-го класса защиты. При установке щитов и ставней с внешней стороны окна, они должны запирается на засов и висячий замок. При высоте окна более 1,5 м щиты и ставни должны запирается на два засова и два замка. Если защита осуществляется с внутренней стороны окна, щиты и ставни запираются только на засовы. Допускается для защиты оконных проёмов использовать рольставни, жалюзи, решётки, которые по прочности и по возможности проникновения через них не уступают требуемому классу защиты.

При установке на оконные проёмы стационарных необрамлённых металлических решёток, концы прутьев необходимо заделывать в стену на глубину не менее 80 мм и заливать цементным раствором или приваривать к металлическим конструкциям.

При установке обрамлённых металлических решёток (обрамление стальным уголком размером не менее 35 x 35 x 4 мм), уголок приваривается по периметру к прочно заделанным в стену на глубину не менее 80 мм стальным анкерам диаметром не менее 12 мм и длиной не менее 120 мм или к закладным деталям. Расстояние между анкерами или закладными деталями должно быть не более 500 мм. Минимальное количество анкеров (закладных деталей) должно быть не менее двух на каждую сторону. Закладные детали изготавливаются из стальной полосы размером 100 x

50 x 6 мм и пристреливаются к стене четырьмя дюбелями. Аналогичным способом крепятся в оконных проёмах и открывающиеся решётки.

## **8. Вентиляционные короба, люки и другие технологические каналы**

Вентиляционные шахты, короба, дымоходы и другие технологические каналы и отверстия диаметром более 200 мм, имеющие выход на крышу или в смежные помещения и своим сечением входящие в помещения, где размещаются материальные ценности, должны быть оборудованы на входе в эти помещения металлическими решётками, выполненными из прутков арматурной стали диаметром не менее 16 мм с размерами ячейки не более чем 150 x 150 мм, сваренной в перекрестиях.

Решётка в венткоробах, шахтах, дымоходах со стороны охраняемого помещения должна отстоять от внутренней поверхности стены (перекрытия) не более чем на 100 мм.

Допускается для защиты вентиляционных шахт, коробов и дымоходов использовать фальшрешётки с ячейкой 100 x 100 мм из металлической трубки с диаметром отверстия не менее 6 мм для протяжки провода шлейфа сигнализации.

В случае прохождения вентиляционных коробов и дымоходов диаметром более 200 мм в стенах помещений объектов подгрупп АI, АII, БII, стены данных помещений с внутренней стороны должны быть укреплены по всей граничащей с коробом (дымоходом) площади стальной решёткой с диаметром прутка не менее 8 мм, с размерами ячейки не более чем 100 x 100 мм, сваренной в перекрестиях.

Двери погрузо-разгрузочных люков по конструкции и прочности должны быть аналогичны ставням, снаружи запираются на висячие (навесные) замки.

Деревянная обвязка погрузо-разгрузочного люка должна крепиться к фундаменту стальными скобами с внутренней стороны или ершами из стали диаметром не менее 16 мм и забиваться в строительные конструкции на глубину не менее 150 мм.

Двери и коробки чердачных люков по конструкции и прочности должны быть аналогичными входным наружным дверям и закрываться изнутри на замки, задвижки, накладки и другие устройства.

В случае наличия на охраняемых объектах неиспользуемых, подвальных помещений, граничащих с помещениями других организаций и собственников, а также арендуемых подвальных помещений, необходимо, при отсутствии двери на выходе из подвального помещения, устанавливать металлическую открывающуюся решетчатую дверь, которая должна закрываться на висячий (навесной) замок.

## **9. Запирающие устройства**

Двери, ворота, люки, ставни, жалюзи и решётки являются надёжной защитой только в том случае, когда на них установлены соответствующие по классу запирающие устройства. Применяют запирающие устройства: врезные, накладные, навесные несамозащёлкивающиеся или самозащёлкивающие замки, задвижки, завёртки, засовы, шпингалеты и т.п.

Висячие (навесные) замки следует применять для запираения ворот, чердачных и подвальных дверей, решёток, ставень и других конструкций. Данные замки должны иметь защитные пластины и кожухи.

Ушки для висячего (навесного) замка должны изготавливаться из стальной полосы сечением не менее 6 x 40 мм.

Цилиндровая часть врезного замка после установки предохранительной накладки, розетки, щитка не должна выступать более чем на 2 мм.

Ключи от замков на оконных решётках и дверях запасных выходов должны размещаться в непосредственной близости или специально выделенном помещении (в помещениях охраны) в ящиках, шкафах или нишах, заблокированных охранной сигнализацией.

Накладные замки должны крепиться к двери болтами. Пропускаемые через дверь болты закрепляются с внутренней стороны помещения при помощи шайб и гаек с расклёпкой конца болта.

## **10. Дополнительные требования к инженерно-технической укрупнённости специальных помещений**

Помещение кассы предприятия и организации должно иметь:

один вход; специальное окно с дверцей для выдачи денег; сейф \_\_\_\_\_ (или металлический шкаф) для хранения денежной наличности и других ценностей.

Дверца специального окна должна соответствовать классу защиты конструкции, в которую она вмонтирована, и закрываться с внутренней стороны на замок и задвижку (шпингалет).

Хранение денежной наличности и других ценностей следует осуществлять в сейфах, при отсутствии сейфа, имеющего сертификат соответствия, допускается хранить денежную наличность и другие ценности в металлических шкафах. В этом случае шкафы или подходы к ним следует защищать охранной сигнализацией.

Сейфы и металлические шкафы массой менее 1000 кг должны крепиться с помощью анкерного крепления к полу или стене либо встраиваться в стену.

Хранение особо ценных и особо важных материальных ценностей следует производить в специально приспособленных для этих целей хранилищах (кладовых) и сейфовых комнатах. Хранилище ценностей должно иметь исполнение, обеспечивающее эффективную защиту от проникновения через железобетонную оболочку (стены, пол, потолок) и дверь с использованием ручного электрифицированного инструмента, домкратов, газорезающего оборудования, взрывчатки, отмычек и иных орудий взлома.

В случае если стены ограждения хранилища, расположенного на первом или втором этажах здания, являются наружными стенами, то между ними и оболочкой хранилища предусматривается смотровой коридор шириной не менее 0,6 м. Смотровые коридоры предусматриваются также и при расположении хранилища на верхних этажах и в подвалах, если на примыкающей к нему наружной стене имеются балконы, карнизы и другие сооружения, позволяющие вести скрытые работы по разрушению стены.

В случае если стены ограждения хранилища являются внутренними стенами здания, за которыми размещаются помещения данной организации, оборудованные охранной сигнализацией, смотровой коридор между стенами ограждения и оболочкой допускается не предусматривать.

При необходимости в качестве запасного аварийного входа в хранилище следует предусматривать люк, размером не менее 500 x 650 мм или диаметром не менее 700 мм. Люк в оболочке хранилища рекомендуется размещать на расстоянии не менее 1 м от бронедвери. Вход в хранилище через люк должен осуществляться из предкладовой.

Наличие окон в хранилище, предкладовой и смотровых коридорах не



допускается.

Вход в помещение сейфовой комнаты должен быть один.

Помещения для хранения гражданского и служебного оружия, боеприпасов, взрывчатых веществ, наркотических средств и психотропных веществ оборудуются в соответствии с требованиями приказов и нормативных документов МВД и МЧС России, регулирующих вопросы их хранения (устанавливаются дополнительные металлические двери из арматуры не менее 16 мм. Диаметр сваренных в перекрестиях ячейками не более 150 мм.).

Помещения охраны объектов подгруппы А1 следует размещать на первом этаже вблизи от главного входа или на КПП. Стены, входные двери, оконные проёмы, запирающие устройства этих помещений должны иметь 3-й класс защиты

При необходимости оконные проёмы помещений охраны следует оснащать удароустойчивым или пулестойким остеклением. При этом должна быть обеспечена непросматриваемость этих помещений снаружи.

**Б 322. В соответствии с государственным стандартом подразделяется пулестойкое стекло (бронестекло) на следующие классы защиты: 1; 2; 2А; 3; 4; 5; 5А; 6; 6А (с защитой вплоть до СВД (снайперская винтовка Драгунова) с боеприпасом 7,62, имеющим специальный наконечник).**

Состав и площади помещений охраны определяются отдельным заданием, согласованным с подразделением ЧОП или ОВО. Помещение охраны должно быть обеспечено телефонной или радиосвязью с дежурным ЧОП или органами внутренних дел.

**Стены, перегородки, потолок и пол помещений оружейных комнат должны быть капитальными:**

- кирпичная или каменная кладка толщиной не менее 360 мм,
- бетонные стеновые блоки толщиной не менее 200 мм,
- бетонные блоки в два слоя, каждый толщиной не менее 90 мм,
- железобетонные панели толщиной не менее 180 мм.

Элементы строения, не отвечающие указанным требованиям, закрываются стальной решеткой, прутья которой должны иметь диаметр или ширину в сечении не менее 16 мм, а размер ячеек – не более 150 x 150 мм.

При возведении внутренних стен допускается их выполнение из спаренных гипсобетонных панелей толщиной не менее 80 мм каждая с проложенной между ними указанной металлической решеткой.

О выполнении указанных требований по техническому укреплению помещений для хранения оружия или патронов составляется акт скрытых работ.

**Вентиляционные люки, отверстия в стенах, предназначенные для инженерных сетей,** закрываются стальной решеткой из прутка диаметром не менее 16 мм с размером ячейки не более 50 x 50 мм.

**Дверные проемы** оборудуются:

- сплошной стальной дверью толщиной не менее 3 мм, усиленной по периметру и диагоналям стальным профилем толщиной стенок не менее 3 мм и шириной полок (сторон) не менее 50 мм;
- решетчатой дверью из прутка диаметром не менее 16 мм с размером ячеек не более 150 x 150 мм, который также приваривается по периметру и диагоналям;
- стальным коробом из профиля с толщиной стенок не менее 5 мм и шириной полок не менее 100 мм.

Вышеуказанные металлические решетки в каждом месте пересечения прутьев и соединения с профилями провариваются, а концы коробов дверных проемов заделываются в стены на 80 мм и цементируются.

**Входная и решетчатая двери** должны иметь внутренние замки, разные по секрету, надежные крепления и устройства петель. Ригели замков или запирающих устройств по площади поперечного сечения должны быть не менее 3 см<sup>2</sup>.

Входная дверь дополнительно оборудуется приспособлениями для опечатывания, а также стальными проушинами толщиной не менее 3 мм для запираения снаружи навесным замком либо вторым внутренним замком.

## **ВОПРОС № 2. ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАННОЙ И ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ**

### **1. Защита периметра территории и открытых площадок**

Технические средства охранной сигнализации периметра должны выбираться в зависимости от вида предполагаемой угрозы объекту, помеховой обстановки, рельефа местности, протяженности и технической укрупненности периметра, типа ограждения, наличия дорог вдоль периметра, зоны отторжения, её ширины.

**Б 328. При использовании технических средств охраны, компьютерной и оргтехники охраннику в части технических требований по их эксплуатации следует руководствоваться: требованиями инструкции предприятий-производителей указанных средств.**

*Охранная сигнализация периметра объекта проектируется, как правило, однорубежной. Выбирают системы которые устойчивы к внешним воздействиям (электромагнитным помехам; сезонным колебаниям температуры; ураганным ветрам, проливным дождям, пыльным бурями; сильным снегопадам и мокрому снегу; метелям и гололёду; частым густым туманам; сейсмическим колебаниям почвы).*

Для усиления охраны, определения направления движения нарушителя, блокировки уязвимых мест следует применять многорубежную охрану.

Технические средства охранной сигнализации периметра могут размещаться на ограждении, зданиях, строениях, сооружениях или в зоне отторжения. Охранные извещатели должны устанавливаться на стенах, специальных столбах или стойках, обеспечивающих отсутствие колебаний, вибраций.

Уязвимые места объекта оснащаются средствами охранной сигнализации и/или средствами охранного телевидения, предназначенными для обнаружения попыток несанкционированного проникновения.

Инженерно-технические меры защиты наиболее уязвимых мест в системе охраны включают установку, эксплуатацию и обслуживание систем и средств охраны. По функциональному назначению инженерно-техническая защита использует следующие средства:

- ⤴ *физические средства защиты, которые включают различные инженерные средства и сооружения, препятствующие физическому проникновению угрозы на объект защиты и осуществляющие защиту персонала, материальных средств, информации от противоправных воздействий;*
- ⤴ *аппаратные средства защиты, куда входят приборы, устройства, приспособления и другие технические решения, препятствующие визуальному наблюдению и дистанционному (стационарному) подслушиванию, защите информации, передаваемой по средствам связи;*
- ⤴ *программные средства защиты. Это специальные программные комплексы и*

### *системы защиты информации в компьютерной сети объекта.*

Одной из эффективных форм обеспечения безопасности объектов является использование технических систем охраны. Технические средства защиты — это разнообразная аппаратура, устройства, приспособления и конструкции, предназначенные для выявления угроз и создания преград на пути их распространения. Применение технических средств позволяет:

- ▲ повысить оперативность действий подразделений охраны за счёт сокращения времени обнаружения проникновения или попытки проникновения на охраняемый объект;
- ▲ повысить надёжность охраны за счёт уменьшения влияния субъективного (человеческого) фактора;
- ▲ в ряде ситуаций реализовать немедленное автоматическое противодействие по фактам нарушения режима охраны;
- ▲ снизить финансовые затраты, за счёт уменьшения численности персонала охраны.

Все технические средства защиты объектов можно разделить на две категории: средства обнаружения и средства противодействия. Охранная сигнализация и охранное телевидение относятся к средствам обнаружения угроз. Заборы и ограждения вокруг территории объекта, решётки на окнах — к средствам противодействия несанкционированному проникновению на охраняемую территорию. Стены, потолки сейфовой комнаты, усиленные двери защищают объект от стихийных бедствий и аварий, служат защитой от подслушивания.

По своему функциональному назначению существующие технические системы подразделяются на:

- ▲ охранную сигнализацию объектов;
- ▲ охранную сигнализацию физических лиц;
- ▲ пожарную сигнализацию;
- ▲ автоматизированный контроль доступа и комбинированные системы.

Технические системы охранно-пожарной сигнализации объектов предназначены для автоматического контроля объекта, регистрации возможных изменений состояния и формирования сигнала тревоги в случае, если отмеченное изменение соответствует попытке нарушения режима охраны.

Охраняемыми объектами могут быть: объекты коммерческих учреждений, административных зданий, промышленных предприятий; объекты торгового назначения, культурно-просветительные учреждения, личное имущество граждан и так далее.

Как правило, оборудуются два рубежа технической охраны в каждой зоне доступности: первый — на размыкание контактов с одновременным включением звуковой и сетевой сигнализации при попытке или проникновении на территорию или в здание. Второй — на основе вещателей объёмного действия в помещениях.

*Технические средства охраны могут иметь демонстративный и скрытый характер.*

Периметр, с входящими в него воротами и калитками, следует разделять на отдельные охраняемые участки (зоны) с подключением их отдельными шлейфами сигнализации к (прибор приёмный контрольный) ППК малой ёмкости или к пульту внутренней охраны, установленных на КПП или в специально выделенном помещении охраны объекта. Длина участка определяется исходя из тактики охраны, технических характеристик аппаратуры, конфигурации внешнего ограждения, условий прямой видимости и рельефа местности, но не более 200 м для удобства технической эксплуатации и оперативности реагирования.

Основные ворота должны выделяться в самостоятельный участок периметра. Запасные ворота, калитки должны входить в тот участок периметра, на котором они находятся.

В качестве пультов внутренней охраны могут использоваться ППК (прибор приёмно-контрольный) средней и большой ёмкости (концентраторы), СПИ (системы передачи извещений), АСПИ (автоматизированные системы передачи извещений) и РСПИ (радиосистемы передачи извещений). Пульты внутренней охраны могут работать как при непосредственном круглосуточном дежурстве персонала на них, так и автономно в режиме "Самоохраны".

Установка охранных извещателей по верху ограждения должна производиться только в случае, если ограждение имеет высоту не менее 2 м.

На КПП, в помещении охраны следует устанавливать технические устройства графического отображения охраняемого периметра (компьютер, световое табло с мнемосхемой охраняемого периметра и другие устройства). Все оборудование, входящее в систему охранной сигнализации периметра должно иметь защиту от вскрытия.

Открытые площадки с материальными ценностями на территории объекта должны иметь предупредительное ограждение и оборудоваться объёмными, поверхностными или линейными извещателями различного принципа действия.

## **2. Защита здания, помещений, отдельных предметов**

Техническими средствами охранной сигнализации должны оборудоваться все помещения с постоянным или временным хранением материальных ценностей, а также все уязвимые места здания (окна, двери, люки, вентиляционные шахты, короба и т.п.), через которые возможно несанкционированное проникновение в помещения объекта.

*Объекты подгрупп АI, АII и БII оборудуются многорубежной системой охранной сигнализации, объекты подгруппы БI - однорубежной.*

**Первым рубежом** охранной сигнализации, в зависимости от вида предполагаемых угроз объекту, блокируют:

- ⤴ деревянные входные двери, погрузочно-разгрузочные люки, ворота - на "открывание" и "разрушение" ("пролом");
- ⤴ остеклённые конструкции - на "открывание" и "разрушение" ("разбитие") стекла; металлические двери, ворота - на "открывание" и "разрушение";
- ⤴ стены, перекрытия и перегородки, не удовлетворяющие требованиям настоящего Руководящего документа или за которыми размещаются помещения других собственников, позволяющие проводить скрытые работы по разрушению стены - на "разрушение" ("пролом");
- ⤴ оболочки хранилищ ценностей - на "разрушение" ("пролом") и "ударное воздействие";
- ⤴ решётки, жалюзи и другие защитные конструкции, установленные с наружной стороны оконного проёма - на "открывание" и "разрушение";
- ⤴ вентиляционные короба, дымоходы, места ввода/вывода коммуникаций сечением более 200 x 200 мм - на "разрушение" ("пролом");

Вместо блокировки остеклённых конструкций на "разрушение", стен, дверей и ворот на "пролом" и "ударное воздействие", допускается, в обоснованных случаях, производить блокировку указанных конструкций только на "проникновение" с помощью объёмных, поверхностных или линейных извещателей различного принципа действия.

При этом следует иметь в виду, что использование в данных целях пассивных оптико-электронных извещателей обеспечивает защиту помещений только от непосредственного проникновения нарушителя.

При невозможности блокировки входных дверей проёмов (тамбуров) техническими средствами раннего обнаружения, необходимо в дверном проёме между основной и дополнительной дверью устанавливать охранные извещатели, обнаруживающие проникновение нарушителя. Данные извещатели следует включать в один шлейф охранной сигнализации блокировки дверей.

Для исключения возможных ложных срабатываний при взятии объекта под охрану указанный шлейф сигнализации необходимо выводить на ППК, имеющий задержку на взятие объекта под охрану.

Извещатели, блокирующие входные двери и неоткрываемые окна помещений, следует включать в разные шлейфы сигнализации, для возможности блокировки окон в дневное время при отключении охранной сигнализации дверей. Извещатели, блокирующие входные двери и открываемые окна допускается включать в один шлейф сигнализации.

К одному прибору приёмно-контрольному (ППК) можно подключить примерно 80 простейших извещателей (СМК) и 50 пожарных извещателей (ИП-104).

**Вторым рубежом** охранной сигнализации защищаются внутренние объёмы и площади помещений на “проникновение” с помощью извещателей различного принципа действия.

В помещениях больших размеров со сложной конфигурацией, требующих применение большого количества извещателей для защиты всего объёма, допускается блокировать только локальные зоны (тамбуры между дверьми, коридоры, подходы к ценностям и другие уязвимые места).

**Третьим рубежом** охранной сигнализации в помещениях защищаются непосредственные места хранения материальных ценностей, блокируются, отдельные предметы: витрины, сейфы, металлические шкафы, в которых сосредоточены ценности и подходы к ним.

*Устанавливаемые в зданиях технические средства охраны должны вписываться в интерьер помещения и по возможности устанавливаться скрыто или маскироваться.*

*В разных рубежах необходимо применять охранные извещатели, работающие на различных физических принципах действия. Основные типы извещателей, обеспечивающие защиту помещений объекта и его конструкций от предполагаемого (возможного) способа криминального воздействия.*

*Количество шлейфов охранной сигнализации должно определяться тактикой охраны, размерами зданий, строений, сооружений, этажностью, количеством уязвимых мест, а также точностью локализации места проникновения для оперативного реагирования на сигналы тревоги.*

*Периметр охраняемого здания, как правило, следует разделять на охраняемые зоны (фасад, тыл, боковые стороны здания, центральный вход и другие участки) с выделением их в самостоятельные шлейфы сигнализации и выдачей отдельных, сигналов на ППК или внутренний пульт охраны объекта.*

Основания задержания и досмотра:

- Когда лицо застигнуто в момент совершения преступления или сразу после его совершения;

- Когда очевидцы, в том числе и потерпевшие прямо укажут на данное лицо;
- Когда на подозреваемом или его одежде, в жилище или при нём будут обнаружены явные следы преступления
- При наличии иных данных (покушение на побег с места происшествия, установки личности как нарушителя или преступника)

### **1-ый рубеж: применяемые извещатели:**

- |                                |                                      |
|--------------------------------|--------------------------------------|
| 1. Контактные                  | - «Фольга», «Провод»                 |
| 2. Магнитоконтактные           | - СМК-1, СМК-3, ИО 102               |
| 3. Ударно-контактные           | - «Окно-4», «Окно-5», «Окно-6»       |
| 4. Звуковые                    | - «Стекло-2», «Стекло-3»             |
| 5. Вибрационные                | - «Шорох1-1»                         |
| 6. Активные оптико-электронные | - «Вектор-2», «Вектор-3», «Рубеж-3М» |
| 7. Пьезоэлектрические          | - «Грань-1», «Грань-2»               |

### **2-ой рубеж: применяемые извещатели:**

- |                                 |                                   |
|---------------------------------|-----------------------------------|
| 1. Объёмные ультразвуковые      | - «Эхо-2», «Эхо-3»                |
| 2. Радиоволновые                | - «Аргус-2», «Аргус-3», «Волна-5» |
| 3. Инфракрасные пассивного типа | - «Фотон»                         |
| 4. Комбинированные              | - «Сокол-2»                       |

### **3-ий рубеж: применяемые извещатели:**

- |                                  |                          |
|----------------------------------|--------------------------|
| 1. Ёмкостные (сейфы, шкафы)      | - «Пик», «Градиент»      |
| 2. Магнитоконтактные (предметы)  | - СМК                    |
| 3. Пьезоэлектрические (предметы) | - «Гюрза-050»            |
| 4. Линейно-электронные (подходы) | - «Вектор-2», «Вектор-3» |

Для усиления охраны и повышения ее надёжности на объектах следует устанавливать дополнительные извещатели - ловушки. Сигналы ловушек выводятся по самостоятельным или, при отсутствии технической возможности, по имеющимся шлейфам охранной сигнализации.

Каждое помещение подгрупп АI и АII должно оборудоваться самостоятельными шлейфами охранной сигнализации. Помещения подгрупп БI и БII, закреплённые за одним материально ответственным лицом, собственником или объединяемые по каким-либо другим признакам также должны оборудоваться самостоятельными шлейфами охранной сигнализации, причём, для удобства эксплуатации, одним шлейфом следует блокировать не более пяти соседних помещений, расположенных на одном этаже.

В помещениях, где круглосуточно должен находиться персонал, охранной сигнализацией должны оборудоваться отдельные участки периметра помещения, а также сейфы и металлические шкафы для хранения ценностей и документов.

### **3. Защита персонала и посетителей объекта**

Для оперативной передачи сообщений на ПЦО и/или в дежурную службу или часть органов внутренних дел, частных охранных структур о противоправных действиях в отношении персонала или посетителей (например, разбойных нападениях, хулиганских действиях, угрозах) объект должен оборудоваться устройствами тревожной сигнализации (ТС): механическими кнопками, радиокнопками, радиобрелоками, педалями, оптико-электронными извещателями и другими устройствами.

*Устройства ТС (тревожной сигнализации) на объекте должны устанавливаться:*

- ✦ *в хранилищах, кладовых, сейфовых комнатах;*
- ✦ *в помещениях хранения оружия и боеприпасов;*
- ✦ *на рабочих местах кассиров;*
- ✦ *на рабочих местах персонала, производящего операции с наркотическими средствами и психотропными веществами;*
- ✦ *в кабинетах руководства организации и главного бухгалтера;*
- ✦ *у центрального входа и запасных выходах в здание; на постах и в помещениях охраны, расположенных в здании, строении, сооружении и на охраняемой территории;*
- ✦ *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 (собственника) объекта или по рекомендации сотрудника вневедомственной охраны.*

*Ручные и ножные устройства ТС (технические средства) должны размещаться в местах, по возможности, незаметных для посетителей. Руководители, ответственные лица, собственники объекта совместно с представителем подразделения вневедомственной охраны определяют места скрытой установки кнопок или педалей тревожной сигнализации на рабочих местах сотрудников.*

Руководство объекта, сотрудников службы безопасности и охраны следует оснащать мобильными устройствами ТС, работающими по радиоканалу (радиокнопками или радиобрелоками).

*Места хранения денежных средств, драгоценных металлов, камней и изделий из них (столы операционно-кассовых работников, металлические шкафы или сейфы, кассовые аппараты, витрины, лотки, торговые прилавки), кроме того, должны быть оборудованы специальными техническими средствами (ловушками), формирующими сигналы тревоги без участия персонала при попытках нарушителя завладеть ценностями. Указанные технические средства должны включаться в шлейфы тревожной сигнализации объекта.*

#### **4. Организация передачи информации о срабатывании сигнализации**

Передача извещений о срабатывании охранной сигнализации с объекта на ПЦО (пульт центральной охраны) может осуществляться с ППК (прибор приёмно-контрольный) малой ёмкости, внутреннего пульта охраны или устройств оконечных СПИ (системы передачи извещений).

Количество рубежей охранной сигнализации, выводимых на ПЦО отдельными номерами, определяется совместным решением руководства объекта и подразделения вневедомственной охраны исходя из категории объекта, анализа риска и потенциальных угроз объекту, возможностей интеграции и документирования ППК (внутренним пультом охраны или устройством оконечным) поступающей информации, а также порядком организации дежурства персонала охраны на объекте.

Минимально необходимое количество рубежей охранной сигнализации, выводимых на ПЦО со всего охраняемого объекта должно быть, для подгруппы:



БI - один объединённый рубеж (первый - периметр)\*;

АI, БII - два объединённых рубежа (первый - периметр и второй - объем)\*.

\* В скобках указано, что все одноименные рубежи охранной сигнализации всех подгрупп охраняемых помещений (кроме специальных помещений), имеющих на объекте, объединяются в соответствующие рубежи и выводятся на отдельные пультовые номера ПЦН ПЦО. Объединение рубежей осуществляется с помощью пультов внутренней охраны, многоточечных (2-х и более) ППК и устройств оконечных.

Кроме того, при наличии на объекте специальных помещений (подгруппа АII, сейфовые, оружейные комнаты и другие помещения, требующие повышенных мер защиты) выводу на ПЦО подлежат также и рубежи охранной сигнализации этих помещений.

При наличии на объекте пульта внутренней охраны с круглосуточным дежурством собственной службы безопасности или частного охранного предприятия, на ПЦО выводятся:

- ⤴ один общий сигнал, объединяющий все рубежи охранной сигнализации объекта за исключением рубежей специальных помещений объекта;
- ⤴ рубежи охранной сигнализации (периметр и объем) специальных помещений.

При этом должна быть обеспечена регистрация всей поступающей информации каждого рубежа охраны помещений на внутреннем пульте охраны.

На объектах, где охраняются только специальные помещения, выводу на ПЦО подлежат все рубежи охранной сигнализации этих помещений.

При охране только отдельных устройств (банкоматы, игровые автоматы, распределительные шкафы и другие аналогичные устройства) на ПЦО выводится один рубеж охранной сигнализации (блокировка на "разрушение" и "вскрытие").

Рубежи охранной сигнализации должны выводиться на ПЦО с пульта внутренней охраны, ППК или устройства оконечного, обеспечивающих запоминание тревожного состояния и его фиксацию на выносном световом (звуковом) оповещателе или индикаторе.

Для объектов жилого сектора допускается применение устройств оконечных и блоков объектовых без соответствующего запоминания тревожного состояния и его фиксации.

Извещения от шлейфов тревожной сигнализации одним объединённым сигналом выводятся на ПЦО и/или в дежурную службу ЧОП непосредственно или через ППК, оконечное устройство СПИ, пульт внутренней охраны.

Извещения охранной и тревожной сигнализации могут передаваться на ПЦО по специально прокладываемым линиям связи, свободным или переключаемым на период охраны телефонным линиям, радиоканалу, занятым телефонным линиям с помощью аппаратуры уплотнения или информаторных СПИ посредством коммутируемого телефонного соединения (метод "автодозвона") с обязательным контролем канала между охраняемым объектом и ПЦО.

С охраняемых объектов "автодозвон" должен осуществляться по двум и более телефонным номерам.

Для исключения доступа посторонних лиц к извещателям, ППК, разветвительным коробкам, другой установленной на объекте аппаратуры охраны должны приниматься меры по их маскировке и скрытой установке. Крышки клеммных колодок данных устройств должны быть опломбированы (опечатаны) электромонтёром ОПС или инженерно-техническим работником подразделения вневедомственной охраны с указанием фамилии и даты в технической документации объекта.

Распределительные шкафы, предназначенные для кроссировки шлейфов

сигнализации, должны закрываться на замок, быть опломбированы и иметь блокировочные (антисаботажные) кнопки, подключённые на отдельные номера пульта внутренней охраны “без права отключения”, а при отсутствии пульта внутренней охраны - на ПЦО в составе тревожной сигнализации.

### **ВОПРОС № 3. СИСТЕМЫ НЕОБХОДИМЫЕ В ОХРАННОЙ ДЕЯТЕЛЬНОСТИ**

#### **1. Системы охранного телевидения**

**Б 314. Основное назначение системы охранного телевидения (СОТ) – это обеспечение передачи визуальной информации о состоянии охраняемых зон, помещений, периметра и территории объекта в помещение охраны. 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, система охранного телевидения позволяет проводить наблюдение охраняемых зон объекта.**

В состав СОТ, согласно ГОСТ Р 51558-2000 входят:

Обязательные устройства для всех СОТ (систем охранного телевидения):

- ♣ передающая телевизионная камера (ТК), камера наблюдения;
- ♣ видеоприёмное устройство, видеомонитор;
- ♣ источник электропитания, в том числе резервный;
- ♣ канал передачи информации (проводной, радио или оптический), линии связи.

Дополнительные устройства для конкретных СОТ:

- ♣ устройство управления и коммутации видеосигналов;
- ♣ обнаружитель движения;
- ♣ видеонакопитель.

На объекте ТК следует оборудовать:

периметр территории;

КПП;

главный и служебные входы;

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

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

другие помещения по усмотрению руководства (собственника) объекта или по рекомендации сотрудника подразделения вневедомственной охраны.

**Б 326. Охранные телевизионные системы в соответствии с требованиями государственных стандартов должны быть устойчивы к несанкционированному доступу к программному обеспечению.**

В охране объектов должны использоваться системы черно-белого и цветного изображения. Установка той или иной системы зависит от необходимой информативности СОТ, характеристик охраняемого объекта (расположение на местности, освещённость и других признаков) и возможных целей (человек, автомобиль и других целей).

Работа аппаратных средств СОТ должна быть синхронизирована.

ТК, предназначенные для контроля территории объекта или ее периметра, должны размещаться в герметичных термокожухах, имеющих солнцезащитный козырёк и должны быть ориентированы на местности под углом к линии горизонта (лучи восходящего и заходящего солнца не должны попадать в объектив ТК). Размещение ТК должно препятствовать их умышленному повреждению.

В тёмное время суток, если освещённость охраняемой зоны ниже чувствительности ТК, объект (зона объекта) должен оборудоваться охранным освещением видимого или инфракрасного диапазона. Зоны охранного освещения должны совпадать с зоной обзора ТК. При использовании СОТ цветного изображения применение инфракрасного освещения недопустимо.

Для наблюдения с помощью одной ТК больших территорий объекта рекомендуется применять объективы с переменным фокусным расстоянием и поворотные устройства с дистанционным управлением.

В помещениях объекта следует использовать ТК с электронным затвором, укомплектованные объективом с ручной регулировкой диафрагмы.

Вне помещений объекта (на улице) следует комплектовать ТК объективом с автоматической регулировкой диафрагмы.

Для отображения поступающей с ТК информации должны применяться специальные мониторы, способные работать круглосуточно в течение длительного времени с неподвижным изображением.

В СОТ следует использовать обнаружители движения, которые превращают ТК в охранный извещатель, выдающий сигнал тревоги на внутренний пульт охраны объекта или ПЦО при появлении в поле зрения ТК движущейся цели.

При необходимости записи телевизионных изображений должны применяться видеонакопители: специальные видеоманитофоны (СВМ) с длительным временем записи или цифровые видеонакопители информации.

Время записи СВМ должно быть не более 24 часов на 3-х часовую видеокассету, время записи на жёсткий диск должно быть не менее 15 дней. Использование СВМ с большим временем записи допускается только при обеспечении автоматического перевода его, в случае поступления извещения о тревоге, в режим записи в реальном времени. Извещение о тревоге может поступать на видеоманитофон от обнаружителя движения или других систем безопасности объекта (охранной, пожарной, тревожной сигнализации и других). Для записи изображения от многих ТК на один видеонакопитель необходимо использовать мультиплексоры.

Время реагирования СОТ на сигнал извещения о тревоге должно быть не более времени, достаточного на преодоление нарушителем,двигающимся со скоростью 3 м/с, половины зоны наблюдения ТК по ширине, в любом месте зоны.

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

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

Конструктивно СОТ должны строиться по модульному принципу и обеспечивать:

- взаимозаменяемость сменных однотипных технических средств;

- удобство технического обслуживания и эксплуатации, а также ремонтпригодность;
- исключение несанкционированного доступа к элементам управления;
- санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

Выбор аппаратуры СОТ его установки и расположения на объекте следует проводить в соответствии с РД 78.36.002-99 и РД 78.36.008-99.

## 2. Системы контроля и управления доступом (СКУД)

В последние годы одним из наиболее эффективных и цивилизованных подходов к решению задачи комплексной безопасности объектов, различных форм собственности является использование систем контроля и управления доступом (СКУД).

**Б 313. Основное назначение системы контроля и управления доступом это обеспечение санкционированного входа и выхода, а также предотвращение несанкционированного прохода в здания, помещения и зоны ограниченного доступа. Правильное использование СКУД позволяет закрыть несанкционированный доступ на территорию, в здание, отдельные этажи и помещения. В то же время они не создают препятствий для прохода персонала и посетителей в разрешённые для них зоны.** Следует помнить, что СКУД не устраняет необходимость контроля со стороны человека, но значительно повышает эффективность работы службы безопасности, особенно при наличии многочисленных зон риска. СКУД освобождает охранников от рутинной работы по идентификации, предоставляя им дополнительное время по выполнению основных функций: охране объекта и защите сотрудников и посетителей от преступных посягательств.

**Системы контроля доступа** – это набор средств видеонаблюдения, которые проводят мониторинг помещений изнутри, а также по периметру объектов. *Системы контроля доступа - это также устройства, препятствующие доступу на территорию нежелательных посетителей. К компонентам систем контроля доступа относятся замки, турникеты, шлагбаумы, а также устройства, открывающие эти механизмы для прохода.*

Назначение системы контроля доступа - это ограничение и разрешение перемещения людей в помещениях, зданиях и по территории охраняемого объекта. Принцип работы системы контроля доступа основан на считывании кодов с идентификаторов и их сравнении с кодами (данными) заложенными в памяти системы, для определения права сотрудника на проход на охраняемую территорию. Основными составляющими системы контроля доступа являются электронные пропуска, которые выдаются сотрудникам охраняемого объекта и считыватели, устанавливаемые у входа в охраняемое помещение, которые распознают код доступа, записанный на электронный пропуск. Если система разрешает доступ, то задействуются дополнительные устройства доступа: турникет, электронный замок и др. Если система не разрешает доступ, включается сигнализация и устройства доступа блокируются.

Системы контроля и управления доступом позволяют осуществлять:

- ✧ ограничение доступа сотрудников и посетителей объекта в охраняемые помещения;
- ✧ временной контроль перемещений сотрудников и посетителей по объекту;

- ♣ *контроль за действиями охраны во время дежурства;*
- ♣ *табельный учёт рабочего времени каждого сотрудника;*
- ♣ *фиксацию времени прихода и ухода посетителей;*
- ♣ *временной и персональный контроль открытия внутренних помещений (когда и кем открыты);*
- ♣ *совместную работу с системами охранно-пожарной сигнализации и телевизионного видеоконтроля (при срабатывании извещателей блокируются или наоборот, например, при пожаре разблокируются двери охраняемого помещения или включается видеокамера);*
- ♣ *регистрацию и выдачу информации о попытках несанкционированного проникновения в охраняемое помещение.*

СКУД обычно состоит из следующих основных компонентов:

- ♣ *устройства идентификации (идентификаторы и считыватели);*
- ♣ *устройства контроля и управления доступом (контроллеры);*
- ♣ *устройства центрального управления (компьютеры);*
- ♣ *устройства исполнительного (замки, приводы дверей, шлагбаумов, турникетов и т.д.).*

В зависимости от применяемой СКУД на объекте, отдельные ее устройства могут быть объединены в один блок (контроллер со считывателем) или вообще отсутствовать (персональный компьютер).

### ***Устройства идентификации доступа***

*Устройство идентификации доступа (идентификаторы и считыватели)* считывает и расшифровывает информацию, записанную на идентификаторах разного типа и устанавливает права людей, имущества, транспорта на перемещение в охраняемой зоне (объекте).

Контролируемые места, где непосредственно осуществляется контроль доступа, например, дверь, турникет, кабина прохода, оборудуются считывателем, устройством исполнительным и другими необходимыми средствами.

*Идентификатор* - предмет, в который (на который) с помощью специальной технологии занесена кодовая информация, подтверждающая полномочность прав его владельца и служащий для управления доступом в охраняемую зону. Идентификаторы могут быть изготовлены в виде карточек, ключей, брелков и т.п.

*Считыватель* - электронное устройство, предназначенное для считывания кодовой информации с идентификатора и преобразования ее в стандартный формат, передаваемый для анализа и принятия решения в контроллер.

Наиболее широкое распространение получили следующие виды идентификаторов и считывателей.

*Карточка перфорированная* - карточка из двухслойной недеформируемой пластмассы. Информация записывается на ней с помощью пробивки специальных отверстий один раз при изготовлении. Считывание информации осуществляется оптическим или механическим считывателями. Данная карточка самый простой и дешёвый тип идентификатора, но который практически не обеспечивает секретность кода и легко подделывается.

*Карточка со штриховым кодом* - карточка с нанесёнными на поверхность

полосами иного цвета, чем остальная поверхность, ширина и расстояние между которыми представляют собой кодовую последовательность. Кодовая последовательность наносится на карточку при ее изготовлении (обычно она определяется генератором случайных чисел), и в дальнейшем не может быть изменена. Код считывается оптическим считывателем (инфракрасным или лазерным). Оптический считыватель не содержит движущихся частей и при сканировании карточки она не контактирует со считывателем физически. Поэтому считыватель надежен в работе и с успехом может применяться вне помещений. Карточка со штриховым кодом может быть пропущена через считыватель в любом направлении. Вероятность подделки карточки такая же как и магнитных.

*Карточка магнитная* - карточка с магнитной полосой, на которой записан код. Данный тип носителя является самоочищающимся и не оставляет окислов на считывателе. При желании код, записанный на дорожках магнитной полосы (Фамилия, Имя, Отчество, место работы, должность, время работы, код допуска, табельный номер) может быть легко перепрограммирован, а при утере карточки можно быстро, дешево и без проблем закодировать новую карточку. Код с карточки считывается магнитным считывателем, принцип работы которого аналогичен считывателю обычного магнитофона: информация считывается при перемещении карточки между магнитными головками считывателя. Карточки с магнитной полосой являются дешёвыми, но не очень надёжными, так как существует вероятность их подделки. К их недостаткам можно также отнести наличие механического контакта при считывании с головками считывателя, который сокращает срок службы (средний срок службы 1 год) и необходимость очень аккуратного обращения, связанного с возможностью искажения или уничтожения записанной информации в относительно слабых магнитных полях и температур окружающего воздуха свыше 80 °С. Размер карточки совпадает с кредитными и банковскими карточками, что позволяет использовать уже имеющуюся у пользователя карточку (например, кредитную) для СКУД. При этом из трех магнитных дорожек одна используется для банковской информации, другая для СКУД и третья для любой другой информации.

*Виганд-карточка* - карточка с содержащимися внутри обрезками тонких металлических проволочек, расположенных в определённом порядке, представляющем собой кодовую комбинацию. Расположение проволочек на карточке фиксируется специальным клеем, после этого переориентация проволочек не возможна. При перемещении данной карточки в магнитном поле считывателя проволочки создают магнитный импульс, несущий информацию, записанную на карточке. Такой тип карточек не подвержен воздействию электромагнитных полей и высоких температур окружающего воздуха. Подделка практически исключена. Считыватели могут работать вне помещений, так как все их электронные компоненты залиты специальным защитным компаундом. Недостатком является то, что карточки хрупкие и могут быть повреждены при изгибе. Кроме того, код каждой карточки записывается в нее при изготовлении и не может быть изменён.

*Карточка бесконтактная (Proximity)* - карточка, внутри которой расположена микросхема (чип) с записанной в ней информацией. Информация с таких карточек считывается радиочастотным способом на расстоянии от 5 до 90 см (для автомобильных идентификаторов данного типа расстояние считывания достигает 2 м). Карточки делятся на активные и пассивные. В пассивных карточках информация записывается один раз на все время действия карточки, а в активных существует возможность изменения информации в микросхеме. Пассивные карточки питаются энергией, получаемой от считывателя, срок службы их неограничен и они не могут быть подделаны. Активные - имеют встроенные, незаменяемые батарейки, срок работы которой обычно достаточно велик - до 10 лет. В надёжности эти карточки уступают

Виганд-карточкам, но они более удобны в применении. Считыватель может быть скрытно размещён за не металлической стенкой. Эта технология идеально сочетает эффективный контроль со свободой перемещения. Информация с карточки может быть считана, даже если она находится в кошельке или кармане. Недостатком является невозможность работы при воздействии сильных электромагнитных полей. Эта карточка незаменима для случаев, когда необходимо обеспечить высокую пропускную способность, скрытность места установки считывателя или дистанционный контроль доступа.

*Электронные ключи «Touch Memory»* выполнены в виде брелков. Все необходимые данные записываются на заключённую в них микросхему. Запись, добавление или стирание ключа осуществляется мастер-ключом из контроллера. Считывается информация при касании ключом считывателя. Микросхема, как правило, питается от вмонтированной в ключ батарейки. Срок ее работы достаточно велик - несколько лет, но рано или поздно ключ подлежит замене. Ключ очень надёжен в работе, устойчив к механическим, электромагнитным воздействиям.

Кроме перечисленных выше могут использоваться идентификаторы следующих типов:

- *с использованием цифровой клавиатуры (PIN-код)*. Носителем информации является пользователь, набирающий на клавиатуре замка личный код (условное число) и, если он верен, то получаете право доступа. Это наиболее простое и дешёвое средство контроля доступа, но которое легко обходится. Хотя, в последнее время, появились клавиатуры, у которых после каждого нажатия, изменяется порядок цифр на клавиатуре по случайному закону, что исключает возможность «подсмотреть» порядок нажатия кнопок или определить наиболее часто используемые кнопки;

- *биометрические* - считывание индивидуальных физических признаков личности (отпечатки пальцев, рисунок ладони, сетчатка глаза, голос и т.д.). Основное преимущество биометрического контроля - это полное решение задачи контроля доступа - идентифицируется личность человека, а не какой-либо предмет (карточка). По причине очень высокой стоимости, малой оперативности и большого объёма машинной памяти, занимаемой одним таким «слепком ключа» они применяются чрезвычайно редко, в основном в учреждениях с повышенной секретностью. Для повышения быстродействия биометрического контроля, как минимум на порядок, совместно с ним используется любой другой способ идентификации.

### **Устройства контроля и управления доступом**

*Контроллеры* - электронные устройства, контролирующие работу считывателей и управляющие устройствами исполнительными. Контроллеры бывают однофункциональными и многофункциональными.

Основное функциональное назначение - это хранение баз данных кодов пользователей, программирование режимов работы, приём и обработка информации от считывателя, принятие решений о доступе на основании поступившей информации, управление исполнительными устройствами и средствами оповещения.

Наиболее существенными дополнительными функциями контроллеров являются:

- защита от повторного использования карточки, т.е. повторный вход по данной карточке возможен только после «ее выхода»;
- наличие и возможности программирования временных зон;
- наличие релейных выходов для подключения средств оповещения, телевизионного оборудования и т.д.;

- возможность подключения охранной сигнализации;
- возможность установки двух и более считывателей на одну дверь для организации двухстороннего прохода или многоуровневого контроля.

На практике применяются контроллеры рассчитанные на управление 1 - 8 считывателями. Все контроллеры, используемые на объекте, в свою очередь могут быть объединены в единую систему и подключаться либо к ведущему контроллеру (мастер-контроллеру), либо к компьютеру, управляющему работой всех контроллеров. Обычно ведущий контроллер отличается от остальных только заложенной программой. К нему же может подключаться управляющий компьютер, принтер и другие периферийные устройства. Однофункциональные контроллеры являются интеллектуальным аналогом кодового замка и работают только в автономном режиме. Многофункциональные контроллеры не только управляют доступом, но и обладают функциями мониторинга состояния устройств исполнительных и вывода данных на компьютер и печать. С помощью многофункциональных контроллеров можно создавать сложные комплексы, интегрированные с другими подсистемами безопасности, например, с охранно-пожарной сигнализацией и телевизионными системами видеоконтроля. Связь контроллеров между собой в единую сеть осуществляется через стандартный интерфейс RS 485. Для связи ведущего контроллера с компьютером используется стандартный интерфейс RS 232. Многофункциональные контроллеры работают в основном в сетевом режиме (централизованный контроль и управление доступом).

### ***Устройства центрального управления***

Персональный компьютер предназначен для программирования СКУД, получения информации о пользователях системы, дате и времени прохода пользователей через контрольные устройства, срабатывании средств охранно-пожарной сигнализации; видеоконтроля, попыток несанкционированного прохода, аварийных ситуациях и т.п.

Для работы в СКУД может использоваться любой персональный IBM-совместимый компьютер. Наряду с работой в составе СКУД он может выполнять и другие функции, т.к. компьютер нужен в основном лишь для программирования системы и получения отчётов о работе системы. Персональный компьютер, используя специально разработанное для охраняемого объекта программное обеспечение (желательно русифицированное), осуществляет общее управление и программирование СКУД, собирает информацию с контроллеров, создаёт общий банк данных, формирует различные отчёты и сводки. Русифицированное программное обеспечение под MS DOS и Windows позволяет осуществлять автоматическую запись данных по всем операциям входа/выхода. В любой момент можно запросить разнообразные сведения, например, о местонахождении сотрудников и посетителей. Текущее состояние СКУД отображается в удобной графической форме. Таким образом, в любой момент времени можно быстро оценить ситуацию и в случае внештатной ситуации оперативно и эффективно принять меры предосторожности.

### ***Устройства исполнительные***

*Устройства исполнительные* системы КУД принимают команды управления с контроллеров и обеспечивают блокировку возможных путей несанкционированного проникновения через устройства заграждения (двери, ворота, турникеты, шлюзовые кабины и т.п.) людей, имущества, транспорта в помещения, здания и на территорию. В устройствах исполнительных применяются исполнительные механизмы электромеханического и электромагнитного принципа действия.



Электромеханический принцип действия исполнительного механизма основан на перемещении закрывающих элементов (запоров, ригелей замков и т.п.) с помощью включения на время их передвижения электромотора или электромагнита. В исполнительных механизмах с электромагнитным принципом действия отсутствуют движущиеся механические закрывающие элементы, т.е. блокировка устройств ограждения, например дверей, осуществляется с помощью сил магнитного притяжения, создаваемых мощным магнитом.

Эти устройства должны отвечать следующим основным требованиям:

- ⤴ должна быть исключена возможность несанкционированного прохода одного лица (или группового прохода) и силового прорыва;
- ⤴ каждые ворота, дверь, дверь шлюза с обеих сторон должны иметь индикаторную панель (один индикатор — замок закрыт, другой индикатор — замок открыт);
- ⤴ должна быть предусмотрена возможность блокировки и разблокировки дверей, ворот, турникетов, работающих в автоматическом режиме, непосредственно с поста охраны в случае нештатной ситуации;
- ⤴ должен быть предусмотрен ручной режим управления с поста охраны (устройств работающих в автоматическом режиме);
- ⤴ пропускная способность исполнительного устройства системы КУД должна обеспечивать нормальное функционирование объекта в течении всего рабочего времени.

### **Критерии оценки системы**

Критериями оценки СКУД являются основные технические характеристики и функциональные возможности. К основным техническим характеристикам относятся:

- уровень идентификации;
- количество контролируемых мест;
- пропускная способность;
- количество пользователей;
- условия эксплуатации.

По уровню идентификации доступа СКУД могут быть:

- **одноуровневые** - идентификация осуществляется по одному признаку, например, по считыванию кода карточки;
- **многоуровневые** - идентификация осуществляется по нескольким признакам, например, по считыванию кода карточки и биометрическим данным.

По техническим характеристикам и функциональным возможностям СКУД условно подразделяются на четыре класса

### **Классы СКУД**

Класс системы	Степень защиты от несанкционированного доступа	Выполняемые функции	Применение
---------------	--	---------------------	------------

Класс системы	Степень защиты от несанкционированного доступа	Выполняемые функции	Применение
1	Недостаточная	<p>Одноуровневые СКУД малой емкости, работающие в автономном режиме и обеспечивающие:</p> <ul style="list-style-type: none"> <li>- допуск в охраняемую зону всех лиц, имеющих соответствующий идентификатор;</li> <li>- встроенную световую/звуковую индикацию режимов работы;</li> <li>- управление (автоматическое или ручное) открытием/закрытием устройства ограждения (например, двери).</li> </ul>	<p>На объектах, где требуется только ограничение доступа посторонних лиц (функция замка).</p>
2	Средняя	<p>Одноуровневые и многоуровневые СКУД малой и средней ёмкости, работающие в автономном или сетевых режимах и обеспечивающие:</p> <ul style="list-style-type: none"> <li>- ограничение допуска в охраняемую зону конкретного лица, группы лиц по дате и временным интервалам в соответствии с имеющимся идентификатором;</li> <li>- автоматическую регистрацию событий в собственном буфере памяти, выдачу тревожных извещений (при несанкционированном проникновении, неправильном наборе кода или взломе ограждающего устройства или его элементов) на внешние оповещатели или внутренний пост охраны;</li> <li>- автоматическое управление открытием/закрытием устройства ограждения.</li> </ul>	<p>То же, что для СКУД 1-го класса.</p> <p>На объектах, где требуется учёт и контроль присутствия сотрудников в разрешённой зоне.</p> <p>В качестве дополнения к имеющимся на объекте системам охраны и защиты.</p>
3	Высокая	<p>Одноуровневые к многоуровневые СКУД средней емкости, работающие в сетевом режиме и обеспечивающие:</p> <ul style="list-style-type: none"> <li>- функции СКУД 2 класса;</li> <li>- контроль перемещений лиц и имущества по охраняемым зонам (объекту);</li> <li>- ведение табельного учета и баз</li> </ul>	<p>То же, что для СКУД 2-го класса.</p> <p>На объектах, где требуется табельный учет и контроль перемещений сотрудников по объекту.</p> <p>Для совместной работы с системами ОПС и ТСВ.</p>

Класс системы	Степень защиты от несанкционированного доступа	Выполняемые функции	Применение
		данных по каждому служащему, непрерывный автоматический контроль исправности составных частей системы;  - интеграцию с системами и средствами ОПС и ТСВ на релейном уровне.	
4	Очень высокая	Многоуровневые СКУД средней и большой емкости, работающие в сетевом режиме и обеспечивающие:  - функции СКУД 3 класса;  - интеграцию с системами и средствами ОПС, ТСВ и другими системами безопасности и управления на программном уровне;  - автоматическое управление устройствами заграждения в случае пожара и других чрезвычайных ситуациях.	То же, что для СКУД 3-го класса.  В интегрированных системах охраны (ИСО) и интегрированных системах безопасности (ИСБ) и управления системами жизнеобеспечения.

### 3. Системы оповещения

**Б 315. Система оповещения на охраняемом объекте и его территории создаётся для оперативного информирования людей о возникшей или приближающейся внештатной ситуации (аварии, пожаре, стихийном бедствии, нападении, террористическом акте) и координации их действий.**

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

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

Эвакуация людей по сигналам оповещения должна сопровождаться:

- включением аварийного освещения;
- передачей специально разработанных текстов, направленных на предотвращение паники и других явлений, усложняющих процесс эвакуации (скопление людей в проходах, тамбурах, на лестничных клетках и других местах);
- включением световых указателей направления и путей эвакуации;

- дистанционным открыванием дверей дополнительных эвакуационных выходов (например, оборудованных электромагнитными замками).

Сигналы оповещения должны отличаться от сигналов другого назначения. Количество оповещателей, их мощность должны обеспечивать необходимую слышимость во всех местах постоянного или временного пребывания людей.

На охраняемой территории следует применять рупорные громкоговорители. Они могут устанавливаться на опорах освещения, стенах зданий и других конструкциях, не должны иметь регуляторов громкости и разъёмных соединений.

Правильность расстановки и количество громкоговорителей на территории определяется расчётом и уточняется на месте экспериментальным путём на разборчивость передаваемых речевых сообщений, но не менее одного 10-ваттного громкоговорителя на каждый участок территории.

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

Управление системой оповещения должно осуществляться из помещения охраны, диспетчерской или другого специального помещения.

#### **4. Системы охранного освещения**

Периметр территории, здания охраняемого объекта должен быть оборудован системой охранного освещения согласно ГОСТ 12.1.046-85.

Охранное освещение должно обеспечивать необходимые условия видимости ограждения территории, периметра здания, зоны отторжения, тропы наряда (путей обхода).

В состав охранного освещения должны входить:

- осветительные приборы;
- кабельные и проводные сети;
- аппаратура управления.

Система охранного освещения должна обеспечивать:

- освещённость горизонтальную на уровне земли или вертикальную на плоскости ограждения, стены не менее 0,5 лк. в тёмное время суток;
- равномерно освещённую сплошную полосу шириной 3 - 4 м;
- возможность автоматического включения дополнительных источников света на отдельном участке (зоне) охраняемой территории (периметра) при срабатывании охранной сигнализации;
- ручное управление работой освещения из помещения КПП, помещения охраны;
- совместимость с техническими средствами охранной сигнализации и охранного телевидения;
- непрерывность работы на КПП, в помещении и на постах охраны.

Сеть охранного освещения по периметру объекта и на территории должна выполняться, отдельно от сети наружного освещения и разделяться на самостоятельные участки в соответствии с участками охранной сигнализации периметра и/или охранного телевидения. Сеть охранного освещения должна подключаться к отдельной группе щита освещения, расположенного в помещении

охраны или на КПП. Допускается установка щита освещения на внешней стене КПП со стороны охраняемой территории. Щит освещения должен быть закрыт на висячий (навесной) замок и заблокирован охранной сигнализацией.

Осветительные приборы охранного освещения могут быть любого типа: подвесные, консольные, прожектора и другие типы. В качестве источника света рекомендуется использовать лампы накаливания напряжением 220 В. При использовании черно-белого охранного телевидения, могут применяться инфракрасные прожекторы для подсветки территории, периметра.

Светильники охранного освещения по периметру территории должны устанавливаться не выше ограждения. Магистральные и распределительные сети охранного освещения территории объекта должны прокладываться, как правило, под землёй или по ограждению в трубах. При невозможности выполнить данные требования воздушные сети охранного освещения должны располагаться достаточно глубоко на территории объекта, чтобы исключить возможность повреждения их из-за ограждения.

В ночное время охранное освещение должно постоянно работать. Дополнительное охранное освещение должно включаться только при нарушении охраняемых участков в ночное время, а при плохой видимости и в дневное.

Лампы охранного освещения должны быть защищены от механических повреждений.

## **5. Система электроснабжения технических средств охраны**

Установленные на объекте технические средства охраны следует относить к 1 категории электроприёмников по надёжности электроснабжения согласно ПУЭ, в силу чего их электропитание должно быть бесперебойным (либо от двух независимых источников переменного тока, либо от одного источника переменного тока с автоматическим переключением в аварийном режиме на резервное питание от аккумуляторных батарей).

Рабочий ввод электропитания, как правило, должен выполняться от электрической сети переменного тока напряжением 220 В.

Резервный ввод электропитания должен выполняться от одного из следующих источников питания или их любых сочетаний:

- ▲ электрической сети переменного тока напряжением 220 В;
- ▲ аккумуляторных батарей;
- ▲ сухих элементов;
- ▲ абонентской телефонной сети.

Электроснабжение технических средств охраны от электрической сети переменного тока осуществляется от отдельной группы электрощита дежурного освещения.

При отсутствии на объекте электрощита дежурного освещения или отдельной группы на нем, заказчик устанавливает самостоятельный электрощит на соответствующее количество групп. Помещение, в котором размещены электрощиты, необходимо оборудовать охранной сигнализацией.

Вне охраняемого помещения электрощиты следует размещать в запираемых металлических шкафах, заблокированных охранной сигнализацией.

Примечание:

При использовании в качестве резервного источника питания аккумуляторной батареи, должна обеспечиваться работа ППК и извещателей охранной и тревожной

сигнализации в течение не менее 24 часов в дежурном режиме и в течение не менее 3 часов в режиме тревоги.

Допускается уменьшать время работы от резервного источника при наличии автоматического или иного оповещения подразделения вневедомственной охраны о моменте отключения основного электропитания:

▲ в городах и посёлках городского типа - до 4 часов в дежурном режиме и до 1 часа в режиме тревоги;

▲ в сельских районах - до 12 часов в дежурном режиме и до 2 часов в режиме тревоги.

Если объект не может быть обеспечен электроснабжением согласно этим требованиям, вопросы электроснабжения решаются и согласовываются с подразделением, вневедомственной охраны в каждом конкретном случае.

После согласования делается соответствующая запись в проектной документации или акте обследования.

Переход технических средств охраны на работу от резервного источника электропитания и обратно должен осуществляться автоматически без выдачи сигналов тревоги.

Линии электропитания, проходящие через незащищаемые охранной сигнализацией помещения, должны быть выполнены скрытым способом или открытым способом в трубах, коробах или металлорукавах.

Линии электропитания технических средств охраны периметра следует выполнять:

- кабелями в траншее, в подземном коллекторе или открыто по внутренней стороне бетонного ограждения (стене здания) бронированными кабелями. В обоснованных случаях допускается прокладка небронированных кабелей (проводов) по внутренней стороне бетонного ограждения (стене здания) в стальных трубах;
- подвеской кабелей на тросе на высоте не менее 3 м или на отдельных участках в охраняемой зоне, при условии защиты кабеля от механических повреждений до высоты 2,5 м.

Соединительные или ответвительные коробки должны устанавливаться в охраняемых помещениях (зонах).

Защитное заземление или зануление технических средств охраны, соединительных и ответвительных коробок и других элементов должно соответствовать требованиям ПУЭ, СНиП 3..05.06-85, РД 78.145-93 (пособия к нему) и технической документации на изделия.

## **6. Системы охранной и охранно-пожарной сигнализации.**

Системы охранно-пожарной сигнализации (ОПС) в том или ином виде используются сегодня практически на всех объектах. Это связано с тем, что использование электроники, в конечном счёте, всегда выгоднее, чем использование охранников.

**Б 310. Система охранной сигнализации определяется, как совокупность совместно действующих технических средств, обнаружения, проникновения (попытки проникновения) на охраняемый объект, сбора, обработки, передачи и представления в заданном виде информации.**

Системы охранно-пожарной сигнализации предназначены для определения факта несанкционированного проникновения на охраняемый объект или появления

признаков пожара, выдачи сигнала тревоги и включения исполнительных устройств (световых и звуковых оповещателей, реле и т. п.). Системы охранной и пожарной сигнализации по идеологии построения очень близки друг другу и на небольших объектах, как правило, бывают совмещены на базе единого контрольного блока - прибора приёмно-контрольного (ППК) или контрольной панели (КП). В целом эти системы включают в себя:

- технические средства обнаружения (извещатели);
- технические средства сбора и обработки информации (приборы приёмно-контрольные, системы передачи извещений и т. п.);
- технические средства оповещения (звуковые и световые оповещатели, модемы и т. п.).

**Технические средства обнаружения** - это датчики (извещатели), построенные на различных физических принципах действия. Извещатель - это устройство, формирующее определённый сигнал при изменении того или иного контролируемого параметра окружающей среды. По области применения извещатели делятся на охранные, охранно-пожарные и пожарные. В настоящее время охранно-пожарные извещатели практически не выпускаются и не применяются.

Технические средства охранной сигнализации предназначаются для обнаружения любых видов угроз, в том числе попыток проникновения на объект, оповещения сотрудников охраны или персонала о появлении угрозы доступа на охраняемую территорию.

*Охранные извещатели по виду контролируемой зоны подразделяются на точечные, линейные, поверхностные и объёмные; по принципу действия подразделяются на электроконтактные, магнитоконтактные, ударноконтактные, пьезоэлектрические, оптико-электронные, ёмкостные, звуковые, ультразвуковые, радиоволновые, комбинированные, совмещённые и др.*

В соответствии с перечисленными функциями в состав технической системы охранной сигнализации входят такие элементы, как датчик, устройства обработки и вывода информации, линии связи.

Датчики (извещатели) как средства обнаружения нарушений режима охраны в значительной степени определяют тактические возможности технической системы охранной, охранно-пожарной и пожарной сигнализации в целом, надёжность обеспечения охраны.

Наиболее важными тактическими характеристиками любого датчика являются:

- ▲ вероятность обнаружения нарушений режима охраны;
- ▲ степень уязвимости;
- ▲ уровень ложных срабатываний.

Датчики являются чувствительными элементами систем, которые воспринимают изменения в состоянии охраняемого объекта и преобразуют их в электрический сигнал.

Любое открывание двери, окна, шкафа, разбитие стекла, пролом стены фиксируются приёмно-контрольным прибором, ведущим непрерывный контроль сигналов установленных датчиков.

Устройство вывода информации выполняет функцию преобразования вида представления информации, то есть сигнал тревоги преобразуется в звуковой, световой или иной сигнал оповещения персонала охраны. Линии связи технических систем охранной сигнализации являются проводными линиями передачи информации.

Охранные датчики (извещатели) подразделяются на два вида — контактные и бесконтактные.

*К контактными относятся:*

**1. Электроконтактные датчики** («Фольга-С», ДЭК-2, ДЭК-3, БК-1М и другие), самый простой тип охранных извещателей. Они представляют собой тонкий металлический проводник (фольга, провод), специальным образом закреплённый на защищаемом предмете или конструкции. Предназначены для защиты строительных конструкций (стекла, двери, люки, ворота, некапитальные перегородки, стены и т.п.) от несанкционированного проникновения через них путём разрушения. Любое физическое действие приводит к разрыву проводника, чем нарушается целостность шлейфа сигнализации.

**2. Магнитоконтактные датчики** (ВК-200, ВК-300, СМК-1, СМК-2, СМК-3 и другие). Диапазон рабочих температур - (минус 40 - +50 °С.), предназначены для подвижных конструкций (распашных, раздвижных, подъёмных ворот, люков) на открывание и выдачу тревожного извещения в виде размыкания электрической цепи шлейфа сигнализации и блокировки различных строительных конструкций (двери, окна, люки, витрины, ворота и т. п.). Магнитоконтактный извещатель состоит из герметизированного магнитоуправляемого контакта (геркона) и магнита в пластмассовом или металлическом немагнитном корпусе. Магнит устанавливается на подвижной (открывающейся) части строительной конструкции (полотно двери, створка окна и т. п.), а магнитоуправляемый контакт - на неподвижной (коробка двери, рама окна и т.п.). Для блокировки больших открывающихся конструкций (раздвижные и распашные ворота), имеющих значительные люфты, применяются электроконтактные извещатели типа путевых конечных выключателей. Их недостаток в том, что их можно «обмануть» при использовании мощного внешнего постоянного магнита.

**3. Ударноконтактные датчики** («ИО 303-1; 3,4,5,» «Окно-2М; 4,5,6», УКД-1М, ВМ-12М, ДИМК и другие). Диапазон рабочих температур - (минус 30 - +50 °С.), предназначены для блокировки различных остеклённых конструкций (окна, витрины, витражи и т.п.) на разбитие. Извещатели состоят из блока обработки сигнала (БОС) и от 5 до 15 датчиков разбития стекла (ДРС). Место расположения составных частей извещателей (БОС и ДРС) определяется количеством, взаимным расположением и площадью блокируемых стеклянных полотен. Принцип действия основан на кратковременном разрыве электрического контакта под действием вибрации от ударов по заблокированной поверхности. Широкое распространение на практике получили ударные датчики на основе *магнитоуправляемых контактов* (постоянный магнит укреплённый на пружинящей пластине, который под действием вибрации начинает раскачиваться и вызывать размыкания и замыкания рядом установленных магнитоуправляемых контактом. Их недостаток — в высоком уровне ложных тревог.

**4. Ртутные датчики** представляют собой запаянный баллончик с расположенными нормально разомкнутыми контактами и небольшим количеством ртути в нижней его части. Принцип действия которых основан на замыкании электроконтактов при перемещении ртути из нижней части баллончика в верхнюю при наклоне. Он реагирует на изменение угла наклона объекта защиты и применяется для обнаружения нарушений через поворачивающиеся фрамуги.

**5. Пьезоэлектрические датчики** (ИО 313-1М, «Шорох -1», «Гюрза-050М», ИО 304-5, «Кристалл», «Грань-2» и другие). Диапазон рабочих температур — (плюс 5 - +40 °С.), используются для блокирования строительных конструкций (стены, пол, потолок и т.п.) и отдельных предметов (сейфы, металлические шкафы, банкоматы и т. п.) различных поверхностей и реагируют на механические колебания этих поверхностей при ударах. Срабатывают на вибрацию или пролом строительных конструкций. Принцип действия датчиков основан на явлении пьезоэлектрического эффекта, так как кристаллы некоторых веществ обладают способностью вырабатывать электрический ток при механическом воздействии на них. предназначены для блокировки При определении



количества извещателей этого типа и места их установки на защищаемой конструкции необходимо учитывать, что возможно использовать их со 100% или 75%-м охватом блокируемой площади. Площадь каждого незащищённого участка блокируемой поверхности не должна превышать 0,1 м<sup>2</sup>.

**6. Проводноволновые датчики** («Уран-1М», «Липа-П», «Плющ», «Газон» и другие) создают объёмную зону обнаружения вокруг чувствительного элемента, который состоит из двух изолированных проводов, проходящих параллельно на расстоянии 0,4-0,5 метра друг от друга и позволяют охранять участки протяжённостью до 200-250 метров. Срабатывает при нарушении или возмущении магнитного поля между проводами.

**7. Вибрационные датчики** («Ежевика», «Лимонник», «Дельфин», «Полынь», «СОС-1» и другие) воспринимают вибрацию (деформацию) элементов сетчатого или решетчатого ограждения, металлической сетки, на которых установлен чувствительный элемент и охраняет участки до 200 метров. Однако они подвержены воздействию таких факторов, как порыв ветра, град, микросейсмическое колебание почвы от проезжающего транспорта.

*К бесконтактным относятся:*

**1. Оптико-электронные датчики** («Вектор-СПЭК», ИО 209-4, «СПЭК-7», «Рубеж-3М», «Окно-4» и другие), реагирующие на механические колебания стеклянных поверхностей, на которых они устанавливаются. подразделяются на активные и пассивные. Активные оптико-электронные извещатели формируют тревожное извещение при изменении отражённого потока (однопозиционные извещатели) или прекращении (изменении) принимаемого потока (двухпозиционные извещатели) энергии инфракрасного излучения, вызванного движением нарушителя в зоне обнаружения. Зона обнаружения таких извещателей имеет вид "лучевого барьера", образованного одним или несколькими расположенными в вертикальной плоскости параллельными узконаправленными лучами. Зоны обнаружения разных извещателей различаются, как правило, длиной и количеством лучей. Конструктивно активные оптико-электронные извещатели, как правило, состоят из двух отдельных блоков - блока излучения (БИ) и блока приёмника (БП), разнесённых на рабочее расстояние (дальность действия).

*Активные* оптико-электронные извещатели применяют для защиты внутренних и внешних периметров, окон, витрин и подступов к отдельным предметам (сейфам, музейным экспонатам и т.п.). *Пассивные* оптико-электронные извещатели имеют наиболее широкое распространение, поскольку, с помощью специально разработанных для них оптических систем (линз Френеля), можно просто и быстро получать зоны обнаружения различной формы и размеров и использовать их для защиты помещений любой конфигурации, строительных конструкций и отдельных предметов.

Принцип действия извещателей основан на регистрации разницы между интенсивностью инфракрасного излучения, исходящего от тела человека, и фоновой температурой окружающей среды. Чувствительным элементом извещателей является пироэлектрический преобразователь (пироприёмник), на котором фокусируется инфракрасное излучение с помощью зеркальной или линзовой оптической системы (последние наиболее широко распространены).

Зона обнаружения извещателя представляет собой пространственную дискретную систему, состоящую из элементарных чувствительных зон в виде лучей, расположенных в один или несколько ярусов или в виде тонких широких пластин, расположенных в вертикальной плоскости (типа "занавес"). Условно зоны обнаружения извещателей можно разделить на семь следующих видов: широкоугольная одноярусная типа "веер"; широкоугольная многоярусная; узконаправленная типа

"занавес", узконаправленная типа "лучевой барьер"; панорамная одноярусная; панорамная многоярусная; конусная многоярусная.

Благодаря возможности формирования зон обнаружения различной конфигурации, пассивные инфракрасные опто-электронные извещатели имеют универсальное применение и могут использоваться для блокировки объёмов помещений, мест сосредоточения ценностей, коридоров, внутренних периметров, проходов между стеллажами, оконных и дверных проёмов, полов, потолков, помещений с наличием мелких животных, складских помещений и т.п.

**2. Ёмкостные датчики** («Риф-М», «Ромб-5», «Сет-11М», «Радан-13», «Пик», «Градиент» и другие). Диапазон рабочих температур - (минус 10 - +50 °С.), предназначены для блокировки металлических шкафов, сейфов, отдельных предметов, создания защитных ограждений. Принцип действия извещателей основан на изменении электрической ёмкости чувствительного элемента (антенны) при приближении или касании человеком охраняемого предмета. При этом охраняемый предмет должен устанавливаться на полу с хорошим изоляционным покрытием или на изолирующей прокладке.

К одному извещателю в помещении допускается подключать несколько металлических сейфов или шкафов. Количество подключаемых предметов зависит от их ёмкости, конструктивных особенностей помещения и уточняется при настройке извещателя.

**3. Фотозлектрические датчики** («Квант-1», Квант-2У», «Вектор-2», «Вектор-3», ДОП-1, ФЭУП и другие) предназначены для защиты охраняемых объектов по внутренним периметрам и создания заградительных барьеров при помощи инфракрасных лучей. Сигнал тревоги формируется извещателями при пересечении нарушителем определённого преграждающего барьера или возникновения в контролируемой зоне задымления.

**4. Ультразвуковые датчики** («Стекло-1; 2,3», ИО 329-1; 2,3,4, «ДУЗ-4», «ДУЗ-5», «Фикус-МП-2» и другие). Диапазон рабочих температур - (+1 - +50 °С.), принцип действия которых основан на регистрации изменений ультразвукового поля, вызванных движением нарушителя или появлением пламени пожара. предназначены для блокировки объёмов закрытых помещений, дальность действия от 1 до 6 метров. Принцип работы извещателей основан на регистрации возмущений поля упругих волн ультразвукового диапазона, создаваемого специальными излучателями, при движении в зоне обнаружения человека. Зона обнаружения извещателя имеет форму эллипсоида вращения или каплевидную форму. Из-за низкой помехоустойчивости в настоящее время практически не используются.

**5. Микроволновые (радиоволновые) датчики** («Фон-1», «Коралл-ДМ» и другие) предназначены для защиты объёмов закрытых помещений, внутренних и внешних периметров, отдельных предметов и строительных конструкций, открытых площадок. Принцип работы радиоволновых извещателей основан на регистрации возмущений электромагнитных волн СВЧ диапазона, излучаемых передатчиком и регистрируемых приёмником извещателя при движении человека в зоне обнаружения. Зона обнаружения извещателя (как и у ультразвуковых извещателей) имеет форму эллипсоида вращения или каплевидную форму, Зоны обнаружения разных извещателей различаются только размерами.

*Радиоволновые извещатели бывают одно- и двухпозиционные.* («Радий-2», «Пион-Т», «Крокус», «Риф-РЛ» и другие). Однопозиционные извещатели применяют для защиты объёмов закрытых помещений и открытых площадок. Двухпозиционные - для защиты периметров.

При выборе, установке и эксплуатации радиоволновых извещателей следует помнить об одной их особенности. Для электромагнитных волн СВЧ диапазона некоторые

строительные материалы и конструкции не являются препятствием (экраном) и они свободно, с некоторым ослаблением, проникают сквозь них. Поэтому зона обнаружения радиоволнового извещателя может выходить, в некоторых случаях, за пределы охраняемого помещения, что может вызвать ложные срабатывания. К таким материалам и конструкциям относятся, например, тонкие гипсокартонные перегородки, окна, деревянные и пластиковые двери и т.п. Поэтому радиоволновые извещатели не следует ориентировать на оконные проёмы, тонкие стены и перегородки, за которыми в период охраны возможно движение крупногабаритных предметов и людей. Не рекомендуется их применять на объектах, вблизи которых расположены мощные радиопередающие средства, принцип действия которых основан на создании поля электромагнитных колебаний и регистрации изменения этого поля при движении объекта.

**6. Инфракрасные датчики** («Диалог», «Рубеж-1М», «Рубеж-3М», «Фотон-1М» и другие) делятся на две группы — активные и пассивные. Активные ИК-датчики используются для формирования одно- или многолучевого барьера с целью защиты периметра охраняемой территории, коридора, многооконного помещения (недостатком является возможность «обмана», если известно расположение лучей). Пассивные ИК-датчики реагируют на внешнее инфракрасное (тепловое) излучение, источником которого является и тепло тела нарушителя (подобные извещатели являются также и пожарными датчиками).

**7.Б 302. Акустические датчики могут применяться в системах охранно-пожарной сигнализации** («Окно-4», «Грань-1» и другие) предназначены для блокировки остеклённых конструкций (окон, витрин, витражей и т.п.) на разбитие. Принцип работы данных извещателей основан на бесконтактном методе акустического контроля разрушения стеклянного полотна по возникающим при его разрушении колебаниям в звуковом диапазоне частот и распространяющихся по воздуху.

При установке извещателя все участки охраняемой остеклённой конструкции должны быть в пределах его прямого обзора. служат для обнаружения вторжения на охраняемый объект по шуму, которым неизбежно сопровождаются подобные попытки. В состав этих датчиков входит микрофон и блок обработки сигналов. При превышении предельно допустимого для охраняемого помещения уровня шума, датчик формирует сигнал тревоги.

**8. Кабельные сигнализационные датчики** («Ворон», «GUARDWIRE» и другие) предназначены для обнаружения несанкционированного вторжения на охраняемые объекты. В качестве чувствительного элемента в системе использовано оптическое волокно, армированное в кабель различной конструкции в зависимости от условий эксплуатации. Оптическое волокно реагирует на незначительные деформации и вибрацию. Кабель закрепляется на любом типе ограждения (забор, сетка «рабица», колючая проволока и др.). Появились извещатели, сочетающие два или несколько принципов действия (ИК пассивный-СВЧ, ИК пассивный-УЗ, СВЧ-УЗ), недостатком комбинированных извещателей является возможность пропуска нарушителя при выходе из строя одного из датчиков.

**9. Комбинированные датчики (извещатели)** представляют собой сочетание двух извещателей, построенных на разных физических принципах обнаружения, объединённых конструктивно и схемно в одном корпусе. Причём схемно они объединены по схеме "и", т. е. *только при срабатывании обоих извещателей формируется тревожное извещение*. Наиболее широко распространена комбинация инфракрасного пассивного и радиоволнового извещателей.

Комбинированные охранные извещатели обладают очень высокой помехоустойчивостью и используются для защиты помещений объектов со сложной

помеховой обстановкой, где применение извещателей других типов невозможно или неэффективно.

**10. Совмещённые датчики (извещатели)** представляют собой два извещателя, построенных на разных физических принципах обнаружения, объединённых конструктивно в одном корпусе. *Каждый извещатель работает независимо от другого и имеет свою зону обнаружения и свой собственный выход для подключения к шлейфу сигнализации.* Наиболее широко распространена комбинация инфракрасных пассивных и звуковых извещателей. Встречаются и другие комбинации.

## **7. Система тревожной сигнализации**

**Б 309. Система тревожной сигнализации определяется, как совокупность совместно действующих технических средств, позволяющих автоматически или вручную выдавать сигнал тревоги на внутренний пульт охраны объекта или на ПЦН (пульт центрального наблюдения) при разбойном нападении, проникновении (попытки проникновения) на охраняемый объект в период его работы.**

В качестве извещателей тревожной сигнализации используются различные кнопки и педали ручного и ножного действия на основе магнито- и электроконтактных извещателей. Как правило, такие извещатели имеют фиксацию в нажатом состоянии и возврат в исходное положение возможен только с помощью ключа.

**Б 312. Система тревожной сигнализации на объекте организуется с использованием принципа – «без права отключения»**

В тех же целях разработаны и применяются специальные мини-системы тревожной сигнализации, работающие по радиоканалу. В их состав входит приёмник, подключаемый к прибору приёмно-контрольному или контрольной панели, и несколько носимых брелоков-передатчиков для беспроводной передачи тревожных извещений.

**Б 330. Переносная тревожная кнопка, использующая радиоканал позволяет охраннику незаметно передавать на приёмно-контрольный прибор сигнализации скрытый сигнал тревоги. В состав некоторых брелоков входит датчик падения.** Дальность действия таких систем составляет от нескольких десятков до нескольких сотен метров.

Особое место среди извещателей тревожной сигнализации занимают извещатели-ловушки. Они предназначены для подачи тревожного извещения при попытке хищения денег или ограбления охраняемого объекта независимо от действий персонала. Они представляют собой имитацию пачки денег в банковской упаковке объёмом 100 купюр, в которую вмонтирован магнит, а в специальную подставку, на которой располагается пачка, магнитный датчик (геркон).

При изъятии (перемещении) имитационной пачки денег с подставки происходит размыкание контактов магнитного датчика и на пульт охраны объекта поступает тревожное извещение. Существуют аналогичные извещатели-ловушки, куда совместно с магнитом встроен специальный патрон, содержащий цветной (оранжевый) дым, объёмом 5 куб. м. Дымовая композиция распыляется с временной задержкой (3 мин.) после срабатывания магнитного датчика.

## **8. Оповещатели применяемые в охранной сигнализации**

**Б 301. В системах охранно-пожарной сигнализации могут применяться среди прочих и световые оповещатели.**

Оповещатели предназначены для подачи световых и звуковых сигналов тревоги, привлечения внимания персонала охраны, психологического воздействия на нарушителя.

В качестве световых оповещателей используются лампы накаливания, светодиоды и импульсные газоразрядные источники света. Устанавливаются внутри помещений удобных для визуального контроля.

В качестве звуковых оповещателей применяются звуковые излучатели различных принципов действия: электромагнитные (сирены, звонки); электродинамические (громкоговорители); пьезоэлектрические. Устанавливаются на улице и высоте не менее 2,5 метра от земли.

## Пожарные извещатели

Пожарные извещатели являются основными элементами автоматических систем пожарной и охранно-пожарной сигнализации.

По способу приведения в действие пожарные извещатели разделяют на ручные и автоматические. В ручных извещателях отсутствует функция обнаружения очага загорания, их действие сводится к передаче тревожного извещения в электрическую цепь шлейфа сигнализации после обнаружения загорания человеком и активизации извещателя путем нажатия соответствующей пусковой кнопки.

Автоматические пожарные извещатели функционируют без участия человека. С их помощью осуществляется обнаружение загорания по одному или нескольким анализируемым признакам и формирование извещения о пожаре при достижении контролируемого физического параметра установленного значения. В качестве контролируемых параметров могут выступать повышенная температура воздуха, выделение продуктов горения, турбулентные потоки горячих газов, электромагнитное излучение и др. В соответствии с обнаруживаемыми первичными признаками пожара извещатели, как уже указывалось ранее, разделяют на *тепловые*, *дымовые*, *пламени*, *газовые* и *комбинированные*. Возможно также использование других признаков пожара. Комбинированные извещатели реагируют на два и более параметра, характеризующих появление очага загорания.

**Дымовые** извещатели реагируют на аэрозольные продукты термического разложения и по принципу действия разделяются на ионизационные и фотоэлектрические. Ионизационные (радиоизотопные) реагируют на тёмный и на светлый дым и имеют низкий процент ложных срабатываний. Фотоэлектрические извещатели линейного типа неплохо реагируют на тёмный и на серый дым и применяются для защиты большой зоны видимости, но не устойчивы к помехам (нуждаются в регулярном техобслуживании) и сравнительно низкая чувствительность к тёмному дыму.

**Тепловые** извещатели реагируют на конвективное тепло от очага пожара, действия их основана на термоэлектрическом эффекте. Пассивные - при достижении максимальной температуры срабатывает термореле (две биметаллические пластины). Активные токопотребляющие выдают информацию о достижении критической температуры и её изменениях.

**Газовые** извещатели реагируют на невидимые газообразные продукты термического разложения если в случае пожара на начальной стадии предполагается выделение определённого вида газа в концентрациях, которые могут вызвать срабатывание извещателей.

**Оптические** извещатели реагируют на оптическое излучение пламени очага пожара и могут использовать метод формирования анализируемого сигнала, позволяющий им реагировать не только на увеличение абсолютного значения температуры выше максимально установленного порога, но и на превышение скорости нарастания ее предельного значения. Поэтому в соответствии с характером реакции на изменение контролируемого признака их разделяют на максимальные, дифференциальные и максимально-дифференциальные.

По способу электропитания пожарные извещатели разделяются на:

- питающиеся по шлейфу сигнализации от прибора приёмно-контрольного или контрольной панели;
- питающиеся от отдельного внешнего источника питания;

- питающиеся от встроенного внутреннего источника питания (автономные пожарные извещатели).

Зона обнаружения извещателя - это пространство вблизи извещателя, в пределах которого гарантируется его срабатывание при возникновении очага загорания. Чаще всего этот параметр выражается в единицах площади (м<sup>2</sup>), контролируемой извещателем с требуемой надёжностью. С увеличением высоты установки извещателя площадь, контролируемая одним извещателем, уменьшается. При высоте установки выше указанной максимальной эффективное обнаружение извещателем очага загорания не гарантируется.

Для световых извещателей защищаемая площадь определяется максимальной дальностью обнаружения открытого тестового очага пожара и углом обзора, зависящим от конструкции оптической системы.

Пожарные извещатели должны обеспечивать надёжное обнаружение очага пожара в конкретных защищаемых помещениях. Для этого при выборе извещателя необходимо учитывать вероятный характер загорания и процесс развития во времени основных факторов пожара: повышения температуры, концентрации дыма, светового излучения в различных точках помещения. В зависимости от вида и количества горючих материалов при пожаре может быть преобладание одного или нескольких обнаруживаемых признаков.

Чаще загорание сопровождается выделением дыма в начальной стадии, поэтому в большинстве случаев наиболее целесообразно применение дымовых извещателей. При выборе дымового извещателя следует учитывать, что ионизационный (радиоизотопный) и оптико-электронный дымовые извещатели имеют разную чувствительность к продуктам горения, частицы дыма которых имеют разный цвет и размеры. Оптико-электронные точечные извещатели лучше реагируют на светлые дымы, характерные для целлюлозосодержащих материалов, а также дымы, состоящие из мелких частиц аэрозоля. Ионизационные извещатели имеют относительно более высокую чувствительность к продуктам горения, выделяющим чёрный дым с более крупными частицами (например, при горении резины).

Помещения, в которых при пожаре наиболее вероятно быстрое появление открытого пламени, предпочтительно оборудовать световыми извещателями.

Тепловые извещатели целесообразно устанавливать, прежде всего, в тех случаях, когда обеспечивается значительная мощность очага пожара и, следовательно, при пожаре будет происходить интенсивное выделение тепла.

При выборе извещателя необходимо учитывать также специальные дополнительные требования к их конструкции и принципу действия. Например, радиоизотопные извещатели не рекомендуется устанавливать в жилых помещениях и детских учреждениях. Во взрывоопасных помещениях должны устанавливаться извещатели, имеющие специальное конструктивное исполнение.

Расчёт общего количества извещателей и определение мест их установки должны проводиться с учётом особенностей помещения, а также требований нормативно-технической документации. К последней относятся соответствующие документы, регламентирующие общие вопросы проектирования и монтажа установок пожарной автоматики, систем и комплексов пожарной и охранной сигнализации, а также эксплуатационная документация на соответствующий тип извещателя.

Все более широкое распространение получают пожарные извещатели, созданные с использованием элементной базы четвёртого поколения: специализированных контроллеров и микропроцессоров. Общей особенностью таких извещателей с расширенными тактико-техническими возможностями является использование для совместной работы только специальных приборов (контрольных

панелей), входящих в состав системы охранно-пожарной сигнализации соответствующей фирмы.

Применение средств вычислительной техники позволяет создавать адресные пожарные извещатели, передающие на центральный процессор контрольной панели информацию о своём местоположении, что обеспечивает точное воссоздание картины и анализ процесса возникновения и развития пожара. Они осуществляют автоматически или по запросу из центра контроль работоспособности и передачу в цифровом виде данных о параметрах своего функционирования. В таких извещателях, при необходимости, возможна подстройка чувствительности при изменении условий внешней среды. Извещатели аналогового типа могут также передавать информацию об уровне контролируемого параметра. Расширение номенклатуры извещателей осуществляется за счёт применения новых технологий. Например, современные зарубежные линейные тепловые извещатели (кабельного типа) улавливают разницу между нормальной и повышенной температурой, что позволяет формировать сигнал тревоги ещё до начала развития пожара (появления дыма или огня) при перегреве контролируемого объекта. Сигнал передаётся в аналоговом виде от извещателя на специальную контрольную панель, которая позволяет определять расстояние до перегретого участка. Такие извещатели могут эффективно применяться для контроля объектов с электрическим оборудованием, помещений с фальшпотолками, кабельных трасс и каналов.

**Пожарные датчики** (ИП-104-1, П-212-9, ДИП-9, РИД-6М и другие) служат для обнаружения возгораний, сопровождающихся появлением дыма в закрытых помещениях, повышения температуры выше 70 градусов по Цельсию. Принцип действия пожарных датчиков основан на размыкании контактных пружин при повышении температуры, так и на эффекте рассеивания оптического излучения аэрозольными продуктами горения.

Действующие нормативные документы: НПБ 88-2001 (Проектирование установок пожаротушения и сигнализации); НПБ 110-03 (Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматической пожарной сигнализацией); РД 78.36.006-2005 (Выбор и применение технических средств охранной, тревожной сигнализации и средств инженерно-технической укрупнённости для оборудования объектов).

### **Приёмно – контрольный прибор**

**Б 303. В большинстве систем охранно-пожарной сигнализации сигнал от охранных датчиков (извещателей) передаётся непосредственно на ПКП (приёмно-контрольный прибор), формирующий сигнал тревоги и рассчитаны на соединение с различными видами датчиков.** Они подразделяются на три группы:

- автономного действия (однолинейного);
- малой ёмкости (многолинейные);
- пульта централизованной охраны.

Приёмно-контрольные приборы (ПКП) являются элементами охранной сигнализации и предназначены для приёма, обработки и фиксации сигналов тревоги, посылаемых датчиками с мест нарушения установленного режима охраны и извещения об этом дежурного состава охраны.

ПКП автономного действия («Сигнал-36», «Сигнал-3М1», «Гамма-2» и другие) позволяют подключать одну линию блокировки с датчиками на объекте.

ПКП (концентраторы) малой ёмкости («Сигнал-12М», «Рубин-2», «Гамма-2» и другие) предназначены для приёма тревожных сообщений от объектовых приборов или датчиков охранной сигнализации и пожарных извещателей и выдачи сигнала тревоги в пункт централизованного наблюдения.



ПКП пульта и системы централизованного наблюдения предназначены для централизованного приёма, обработки и воспроизведения информации с объектов охраны. Они обеспечивают:

- контроль состояния охраняемых объектов, взятие и снятие объектов с охраны;
- автоматическое переключение аппаратуры АТС на аппаратуру систем на время охраны;
- регистрацию нарушения шлейфов охраняемых объектов с указанием номера объекта и характера нарушения; световую индикацию номеров объектов, на которых произошло нарушение.

*К системе защиты относятся технические средства наблюдения, а также средства поисковой техники.* Технические средства наблюдения делятся на:

- оптико-механические (бинокли, оптические прицелы и другие);
- радиолокационные приборы, используемые для определения скорости движущихся транспортных средств («Радар», «Барьер» и другие);
- электронно-оптические приборы (приборы ночного видения и другие)

## **Средства поисковой техники применяемой в охранной деятельности.**

Средства поисковой техники делятся на три группы:

1. **контактные** (обнаруживают искомый объект при непосредственном механическом контакте с ним — щупы, **для осмотра труднодоступных внутренних плоскостей различных предметов применяются технические эндоскопы** .Б 316);

2. **неконтактные** (к ним относятся металлоискатели, металлодетекторы

**(для скрытного распознавания наличия оружия на расстоянии до 70 см. применяется скрытноносимый селективный металлодетектор АКА 7220 с сигналом оповещения по радиоканалу Б 329), индикаторы неоднородностей (газоанализаторы), рентгеновские установки (нелинейные локаторы, рентгено-просмотровая техника,**

**для обеспечения безопасного поиска ферромагнитных предметов (чёрных металлов в условиях возможного наличия взрывных устройств с электронной схемой подрыва) применяются магнитометрические поисковые приборы** Б 317)

3. **вспомогательные** (включают приборы ультрафиолетовой и инфракрасной техники, например, «Рельеф», «Квадрат», УМ-1, ОЛД-41 и другие).

Охранная и пожарная сигнализации используют однотипные элементы (каналы связи, тревожное оповещение, радиосвязь и энергоснабжение).

## **ВОПРОС № 4. ТЕХНИЧЕСКИЕ СРЕДСТВА СБОРА И ОБРАБОТКИ ИНФОРМАЦИИ.**

К техническим средствам сбора и обработки информации относятся приборы приёмно-контрольные, контрольные панели, сигнально-пусковые устройства, системы передачи извещений и т.п. Они предназначены для непрерывного сбора информации от технических средств обнаружения (извещателей), включённых в шлейфы сигнализации, анализа тревожной ситуации на объекте и ее отображения, управления местными световыми и звуковыми оповещателями, индикаторами и другими устройствами (реле, модем, передатчик и т. п.), а также формирования и передачи извещений о состоянии объекта на центральный пост или пульт централизованного наблюдения. Они же обеспечивают сдачу под охрану и снятие

объекта (помещения) с охраны по принятой тактике, а также в ряде случаев электропитание извещателей. Извещатели (датчики) предназначены для обнаружения разрушения, проникновения в охраняемые зоны и помещения и выдачи тревожного извещения (сигнала) в шлейф охранной сигнализации приёмно-контрольных приборов УОТС-1-1, УОТС-М, УОТС-А, «Сигнал-45», «Рубин-3», «Рубин-6», «Топаз», «Буг»

Приборы приёмно-контрольные классифицируются по информационной ёмкости (количеству контролируемых шлейфом сигнализации) на приборы малой (до 5 ШС), средней (от 6 до 50 ШС) и большой (свыше 50 ШС) информационной ёмкости. По информативности приборы могут быть малой (до 2-х видов извещений), средней (от 3 до 5 видов) и большой (свыше 5 видов) информативности.

Системы передачи извещений классифицируются по информационной ёмкости (количеству охраняемых объектов) на системы с постоянной информационной ёмкостью и с возможностью наращивания информационной ёмкости.

По информативности системы подразделяются на системы малой (до 2-х видов извещений), средней (от 3 до 5 видов) и большой (свыше 5) информативности.

По типу используемых линий (каналов) связи системы подразделяются на системы, использующие линии телефонной сети (в том числе переключаемые), специальные линии связи, радиоканалы, комбинированные линии связи и др.

По количеству направлений передачи информации они подразделяются на системы с одной- и двунаправленной передачей информации (с наличием обратного канала).

По алгоритму обслуживания объектов системы передачи сообщений подразделяются на не автоматизированные системы с ручной тактикой взятия (снятия) объектов под охрану (с охраны) после ведения телефонных переговоров с дежурным пультом управления и автоматизированные с автоматическим взятием и снятием (без ведения телефонных переговоров).

По способу отображения поступающей на пульт централизованного наблюдения информации системы передачи извещений подразделяются на системы с индивидуальным или групповым отображением информации в виде световых и звуковых сигналов, с отображением информации на дисплее с применением устройств обработки и накопления базы данных.

Контрольные панели по основным решаемым задачам соответствуют отечественным приборам приёмно-контрольным. Уточним также понятия зоны охраны (термин, применяемый в иностранной литературе) и шлейфа сигнализации, используемого в отечественной литературе. Сразу же отметим, что эти понятия разные.

#### 4.1 Виды помех и их возможные источники

Извещатели в процессе эксплуатации подвергаются воздействию различных мешающих факторов, среди которых основными являются: акустические помехи и шумы, вибрации строительных конструкций, движение воздуха, электромагнитные помехи, изменения температуры и влажности окружающей среды, техническая неукреплённость охраняемого объекта.

Степень воздействия помех зависит от их мощности, а также от принципа действия извещателя.

**Акустические помехи и шумы создаются промышленными установками, транспортными средствами, бытовой радиоаппаратурой, грозowymi разрядами и другими источниками.** Примеры акустических помех приведены в **таблице 1**.

Таблица 1. Примеры акустических помех

Сила звука, дБ	Примеры звуков указанной силы
0	Предел чувствительности человеческого уха.
10	Шорох листьев. Слабый шёпот на расстоянии 1 м.
20	Тихий сад.
30	Тихая комната. Средний уровень шума в зрительном зале.
40	Негромкая музыка. Шум в жилом помещении.
50	Слабая работа громкоговорителя. Шум в учреждении с открытыми окнами.
60	Громкий радиоприёмник. Шум в магазине. Средний уровень в разговорной речи на расстоянии 1 м.
70	Шум мотора грузового автомобиля. Шум внутри трамвая.
80	Шумная улица. Машинописное бюро.
90	Автомобильный гудок.
100	Автомобильная сирена. Отбойный молоток.
120	Сильные удары грома. Реактивный двигатель.
130	Болевой предел. Звук уже не слышен.

Этот вид помех вызывает появление неоднородностей воздушной среды, колебания не жёстко закреплённых остеклённых конструкций и может служить причиной ложных срабатываний ультразвуковых, звуковых, ударноконтактных и пьезоэлектрических извещателей. Кроме того, на работу ультразвуковых извещателей оказывают влияние высокочастотные составляющие акустических шумов.

**Вибрации строительных конструкций вызываются железнодорожными составами и поездами метрополитена, мощными компрессорными установками и т.п. Особенно чувствительны к вибрационным помехам ударноконтактные и пьезоэлектрические извещатели, поэтому на объектах, подверженных таким помехам, эти извещатели применять не рекомендуется.**

**Движение воздуха в охраняемой зоне вызывается, в основном, тепловыми потоками вблизи отопительных устройств, сквозняками, вентиляторами и т.п. Наиболее подвержены влиянию воздушных потоков ультразвуковые и пассивные**

*оптико-электронные извещатели. Поэтому эти извещатели не следует устанавливать в местах с заметным движением воздуха (в оконных проёмах, около батарей центрального отопления, около вентиляционных отверстий и т. п.).*

**Электромагнитные помехи** создаются грозowymi разрядами, мощными радиопередающими средствами, высоковольтными линиями электропередач, распределительными сетями электропитания, контактными сетями электротранспорта, установками для научных исследований, технологических целей и т.п.

Наиболее подвержены воздействию электромагнитных помех радиоволновые извещатели. Причём в большей степени они восприимчивы к радиопомехам. Наиболее опасными электромагнитными помехами являются помехи из сети электропитания. Они возникают при коммутации мощных нагрузок и могут проникать во входные цепи аппаратуры через вводы силового питания, вызывая ее ложные срабатывания. Существенное уменьшение их количества даёт применение и своевременное техническое обслуживание источников резервного питания.

Исключить воздействие электромагнитных помех сетей переменного тока на работу извещателей позволяет соблюдение основного требования по монтажу низковольтных соединительных линий: прокладка линий питания извещателя и ШС должна проводиться параллельно силовым сетям на расстоянии между ними не менее 50 см, а их пересечение должно производиться под прямым углом.

**Изменения температуры и влажности окружающей среды на охраняемом объекте** могут оказывать влияние на работу ультразвуковых извещателей. Это обусловлено тем, что поглощение ультразвуковых колебаний в воздухе в сильной степени зависит от его температуры и влажности. Например, при повышении температуры среды от +10 до +30 °С коэффициент поглощения возрастает в 2,5-3 раза, а при повышении влажности от 20-30% до 98% и понижении ее до 10% коэффициент поглощения изменяется в 3-4 раза.

Уменьшение температуры на объекте в ночное время по сравнению с дневным приводит к уменьшению коэффициента поглощения ультразвуковых колебаний и, как следствие, к увеличению чувствительности извещателя. Поэтому, если регулировка извещателя производилась в дневное время, в ночное время в зону обнаружения могут попасть источники помех, которые в период регулировки находились вне этой зоны, что может вызвать срабатывание извещателя.

**Техническая неукреплённость объектов** оказывает значительное влияние на устойчивость работы магнитоконтактных извещателей, применяемых для блокировки элементов строительных конструкций (дверей, окон, фрамуг и т.п.) на открывание. Кроме того, плохая техническая укрепленность может служить причиной ложных срабатываний других извещателей за счёт сквозняков, вибраций остеклённых конструкций и т. п.

Следует отметить, что существует ряд специфических факторов, вызывающих ложные срабатывания извещателей только определённой категории. К ним относятся: движение мелких животных и насекомых, люминесцентное освещение, радиопроницаемость элементов строительных конструкций, попадание на извещатели прямых солнечных лучей и света автомобильных фар.

**Движение мелких животных и насекомых** может восприниматься как движение нарушителя извещателями, принцип действия которых основан на эффекте Доплера. К ним относятся ультразвуковые и радиоволновые извещатели. Влияние ползающих насекомых на извещатели можно исключить обработкой мест их установки специальными химическими средствами.

При использовании на объекте, охраняемом радиоволновыми извещателями, люминесцентного освещения источником помех являются мигающий с частотой 100 Гц столб ионизированного газа лампы и вибрация арматуры лампы с частотой 50 Гц.

Кроме этого, люминесцентные и неоновые лампы создают непрерывные флуктуационные помехи, а ртутные и натриевые лампы - импульсные помехи с широким спектром частот. Например, люминесцентные лампы могут создавать

значительные радиопомехи в полосе частот 10 -100 МГц и более.

Дальность обнаружения таких источников света всего в 3-5 раз меньше дальности обнаружения человека, поэтому на период охраны их необходимо выключать, а в качестве дежурного освещения использовать лампы накаливания.

**Радиопроницаемость элементов строительных конструкций** также может стать причиной ложного срабатывания радиоволнового извещателя, если стены имеют малую толщину или в них имеются значительные по размерам тонкостенные проёмы, окна, двери.

Энергия, излучаемая извещателем, может выходить за пределы помещения, при этом извещатель обнаруживает проходящих снаружи людей, а также проезжающий транспорт. Примеры радиопроницаемости строительных конструкций приведены в **таблице 2**.

Таблица 2. Примеры радиопроницаемости строительных конструкций

Элемент конструкции	Толщина, см	Ослабление, раз
Железобетонная стена	40	1000
Межэтажное перекрытие	-	160
Кирпичная стена	70	120
Шлакобетонная стена	46	110
Окно с двойной рамой	-	20
Оштукатуренная панель	15	16

**Тепловое излучение осветительных приборов** может служить причиной ложных срабатываний пассивных оптико-электронных извещателей. Это излучение по мощности соизмеримо с тепловым излучением человека и может служить причиной срабатывания извещателей.

В целях исключения воздействия этих помех на пассивные оптико-электронные извещатели можно рекомендовать изоляцию зоны обнаружения от воздействия излучения осветительных приборов. Уменьшение влияния мешающих факторов, а, следовательно, и снижение количества ложных срабатываний извещателей, в основном, достигается соблюдением требований к размещению извещателей и их оптимальной настройкой по месту установки.

## ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА

1. Закон РФ № 298-ФЗ «О частной детективной и охранной деятельности в Российской Федерации» (01.03.2011 г. вступила в силу новая редакция) М. 15.11.2010г.
2. РД 78.36.003-2002 и РД 78.36.032-2013 г. "Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств" Москва 2013 г.
3. С.Д. Анцифиров Специальная подготовка частных охранников Москва 2004г.
4. В.В. Черняев Тактика охраны различных объектов Москва 2007г.
5. П.А. Гнесь Тактика охранной деятельности С.Пб 1998г.
1. С.Н. Федоткин Основы частной охранной деятельности Москва «Мир безопасности» 2001г.
6. НПБ 85-200 «Извещатели пожарные тепловые. Технические требования пожарной безопасности. Методы испытаний» Москва 2001 г.
7. В.Г. Синилов «Системы охранной, пожарной и охранно-пожарной сигнализации» профОбриЗдат Москва 2001 г.
8. С.Ф. Радвила «Применение технических средств в борьбе с терроризмом» НИЦ «охрана» Москва 2000 г.

*Составил:*

*Е.А. Крутов*