ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесенных к 2, 3 и 4 категориям. Методические рекомендации

Р 78.36.059-2016

Москва 2016

gost.e-ecolog.ru

Методические рекомендации разработаны сотрудниками ФКУ «НИЦ «Охрана» к.т.н. С.Л. Цыцуриным, И.В. Морозом, Н.А. Федоровым, Н.П. Ивановым, В.В. Стецким, под руководством к.т.н. А.Г. Зайцева.

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесенных к 2, 3 и 4 категориям. Методические рекомендации»: Методические рекомендации (Р 78.36.059-2016). – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2016. – 386 с.

Методические рекомендации предназначены для использования в служебной деятельности сотрудниками инженерно-технической службы ГУВО Росгвардии, подразделений вневедомственной охраны полиции, специалистами ФГУП «Охрана» Росгвардии.

ВВЕДЕНЫ
С 1 января 2017 г.

© ФКУ «НИЦ «Охрана» Росгвардии, 2016

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казённое учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых ко второй категории»

Москва 2016 г.

СОДЕРЖАНИЕ

№ раздела	Наименование системы	№ листов
1	Система охранно-тревожной сигнализации.	3-57
2	Система охранная телевизионная.	58-95
3	Система контроля и управления доступом.	96-133

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых ко второй категории»

Система охранно-тревожной сигнализации

РАЗДЕЛ 1

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	6
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	8
3.	СИСТЕМА ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ (СОТС)	8
3.1	Назначение СОТС	8
3.2	Состав СОТС	9
3.3	Средства обнаружения проникновения	9
3.4	Критерии выбора СОТС	25
3.5	Организация передачи информации на пульт централизованного наблюдения (ПЦН)	25
3.6	Электропитание	27
3.7	Общие требования к минимально необходимому составу СОТС	29

ПРИЛОЖЕНИЯ

Приложение 1.	Условные обозначения.	35
Приложение 2.	Схема блокировки двери, окна извещателем охранным магнитоконтактным.	36
Приложение 3.	Схема установки извещателя охранного ударно-контактного для блокировки окна.	37
Приложение 4.	Схема установки извещателя охранного поверхностного звукового (акустического).	38
Приложение 5.	Схема установки извещателя охранного поверхностного оптико-электронного (инфракрасного).	39
Приложение 6.	Схема установки извещателя охранного объёмного ультразвукового.	40
Приложение 7.	Схема установки извещателя охранного объёмного радиоволнового.	41
Приложение 8.	Схема установки извещателя охранного объёмного оптико-электронного (инфракрасного).	42
Приложение 9.	Схема установки извещателя охранного поверхностного вибрационного на стене.	43
Приложение 10.	Схема установки извещателя охранного поверхностного вибрационного с датчиком наклона.	44
Приложение 11.	Схема установки извещателя охранного поверхностного вибрационного для охраны немонолитной (многосекционной) конструкции.	45
Приложение 12.	Схема установки извещателя охранного объёмного совмещённого (ИК+АК).	46

Приложение 13.	Схема установки извещателя охранного поверхностного совмещённого (ИК+АК).	47
Приложение 14.	План расположения оборудования СОТС комнаты хранения оружия.	48
Приложение 15.	Комната хранения оружия. Схема структурная.	49
Приложение 16.	План расположения оборудования СОТС 1-го этажа здания ОВД.	50
Приложение 17.	План расположения оборудования СОТС 2-го этажа здания ОВД.	51
Приложение 18.	План расположения оборудования СОТС 1-го этажа здания ЛОВД.	52
Приложение 19.	План расположения оборудования СОТС 2-го этажа здания ЛОВД.	53
Приложение 20.	План расположения оборудования СОТС 3-го этажа здания ЛОВД.	54
Приложение 21.	План расположения оборудования СОТС 4-го этажа здания ЛОВД.	55
Приложение 22.	Схема блокировки венткороба омическим извещателем.	56
Приложение 23.	Схема блокировки окна омическим извещателем.	57

1. ОБЩАЯ ЧАСТЬ

Методические рекомендации по оснащению ведомственных объектов СОТС разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 2 января 2013 г. № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;

- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- ГОСТ Р 50658-94 (МЭК 60839-2-4:1990) «Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений»;
- ГОСТ Р 50659-12 «Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний»;
- ГОСТ Р 50777-14 «Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний»;
- ГОСТ Р 51186-98 «Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний»;
- Р 78.36.018–2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- Р 78.36.019–2012 «Рекомендации по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий»;
- Р 78.36.026-2012 «Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны ограждённых территорий и открытых площадок»;
- Р 78.36.028-2012 «Рекомендации. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов»;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану. Методические рекомендации»;
- Р 78.36.032-2013 «Инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1»;

- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения»;
- Р 78.36.050-2015 «Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних периметров, дверей, окон, витрин и подступов к отдельным предметам»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

В соответствии с пунктом 4.2 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом II категории по степени потенциальной угрозы понимается обособленное помещение или группа помещений, расположенных в зданиях или сооружениях, не относящихся к системе органов внутренних дел Российской Федерации, в которых внутриобъектовый режим требует осуществления пропускного режима и круглосуточного дежурства.

3. СИСТЕМА ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ

3.1 Назначение системы охранно-тревожной сигнализации.

СОТС – это 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.

При выборе технических средств охраны, для оборудования объекта СОТС рекомендуется применять приборы, указанные в «Списке технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны,

предназначенным для применения в подразделениях вневедомственной охраны» (действующая редакция).

3.2 Состав СОТС.

СОТС включает в себя:
- средства обнаружения проникновения (охранные извещатели);
- средства тревожной сигнализации (СТС);
- приборы приёмно-контрольные (ППК), и охранно-пожарные (ППКОП), устройство оконечное объектовое (УОО) системы передачи извещений (СПИ);
- средства оповещения (оповещатели световые, звуковые, комбинированные светозвуковые);
- СПИ на пульт централизованного наблюдения (ПЦН);
- источники вторичного электропитания (ИВЭП).

3.3 Средства обнаружения проникновения.

3.3.1 Классификация средств обнаружения проникновения.

Средства обнаружения проникновения (охранные извещатели), предназначенные для применения на объектах, классифицируют по следующим признакам функционального назначения.

3.3.1.1 По способу приведения в действие:
- автоматические;
- ручные (ножные).

3.3.1.2 По условиям эксплуатации:
- в отапливаемых помещениях;
- в помещениях с нерегулируемыми и неконтролируемыми параметрами температуры и влажности воздуха (в том числе под навесами);
- для эксплуатации на открытом воздухе.

3.3.1.3 По виду зоны, контролируемой автоматическим извещателем:
- точечные;
- линейные;
- поверхностные;
- объёмные.

3.3.1.4 По физическим принципам, положенным в основу обнаружения:
- электроконтактные;
- магнитоконтактные;
- ударноконтактные;
- ёмкостные;
- радиоволновые;

– оптико-электронные;
– вибрационные;
– звуковые (акустические).

3.3.1.5 По способу электропитания – на обеспечиваемые электропитанием от:

– источника постоянного тока;
– сети переменного тока;
– шлейфа сигнализации охранного приемно-контрольного прибора или оконечного объектового устройства системы передачи извещений;
– автономных источников.

3.3.1.6 По сочетанию принципов обнаружения:

– использующие один физический принцип;
– использующие два и более физических принципа: комбинированные, совмещенные.

3.3.2 Типы средств обнаружения, их назначение и функции.

Существует 12 типов средств обнаружения проникновений и угроз различных видов:

– магнитоконтактные извещатели для блокировки дверных, оконных конструкций и отдельных предметов;
– ударно-контактные извещатели для блокировки остеклённых конструкций;
– звуковые (акустические) извещатели для блокировки остеклённых конструкций;
– вибрационные извещатели для блокировки строительных конструкций и сейфов;
– ультразвуковые извещатели для блокировки объёма помещений;
– оптико-электронные пассивные извещатели для блокировки объема помещений;
– оптико-электронные активные извещатели для блокировки проёмов помещений и отдельных предметов;
– радиоволновые извещатели для блокировки объема помещений;
– ёмкостные извещатели для блокировки отдельных предметов;
– комбинированные извещатели для блокировки объема помещений;
– совмещённые извещатели для блокировки объема помещений и остеклённых конструкций;
– извещатели тревожной сигнализации (тревожные кнопки, педали).

3.3.2.1. Магнитоконтактные извещатели (Рисунок 1-4).

Магнитоконтактные извещатели применяют для блокировки «на открывание» подвижных строительных конструкций (дверей, окон, фрамуг, люков, ворот, т.п.), а также для блокировки «на перемещение» предметов (музейных или выставочных экспонатов, картин, товаров на витринах и стеллажах и т.п.).

Магнитоконтактные извещатели конструктивно состоят из двух частей: исполнительного блока (магнитоуправляемого датчика на основе геркона) и задающего блока, заключенного в отдельный корпус из «немагнитных» материалов (пластик, алюминий) управляющего элемента. В качестве управляющего элемента используют постоянный магнит, фрагмент магнитопровода или магнитопровод самой защитной конструкции.

Исполнительный блок извещателя устанавливают на неподвижную часть охраняемой конструкции, задающий блок – на перемещаемую (открываемую, сдвигаемую, наклоняемую) часть охраняемой конструкции.

Эти извещатели выдают извещение о тревоге посредством размыкания контактов встроенного геркона.

В зависимости от конструктивного исполнения магнитоконтактные извещатели подразделяют:

- для открытой установки на поверхности охраняемой конструкции;
- для скрытой установки в охраняемую конструкцию.



Рисунок 1. Магнитоконтактный извещатель для блокировки дверных, оконных конструкций и отдельных предметов.



Рисунок 2. Магнитоконтактный извещатель для открытого монтажа на конструкциях, выполненных из магнитных материалов.



Рисунок 3. Магнитоконтактный извещатель для скрытого монтажа на конструкциях, выполненных из немагнитных материалов.



Рисунок 4. Магнитоконтактный извещатель для скрытого монтажа на конструкциях, выполненных из магнитных материалов.

Сигнал «тревога» данные извещатели выдают посредством размыкания контактов встроенного геркона.

В зависимости от конструктивного исполнения магнитоконтактные извещатели подразделяют на датчики, предназначенные для открытой установки на поверхности охраняемой конструкции и для скрытой установки в охраняемую конструкцию.

3.3.2.2 Концевые выключатели.

Концевые выключатели конструктивно состоят из одного блока, применяются для блокировки ворот, люков на открывание (Рисунок 5).



Рисунок 5. Концевой выключатель.

3.3.2.3 Ударно-контактные извещатели (Рисунок 6).

Ударно-контактные извещатели предназначены для использования в составе систем охранной сигнализации с целью обнаружения разрушения установленного в строительной конструкции стекла или стеклопакета при попытке нарушителя проникнуть в защищаемое помещение через эту остекленную конструкцию.

Ударно-контактные извещатели состоят из блока обработки сигналов (БОС) и комплекта миниатюрных датчиков разрушения стекла, устанавливаемых непосредственно на стекла, охраняемые извещателем.

В ударно-контактных извещателях срабатывание геркона происходит под воздействием вибрационных колебаний определенной амплитуды, длительности и направления распространения, возникающих при разрушении стекла.

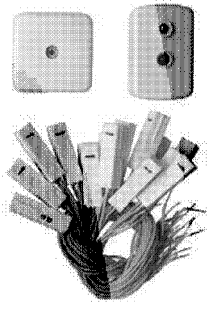


Рисунок 6. Ударно-контактные извещатели для остеклённых конструкций.

3.3.2.4 Извещатели охранные поверхностные звуковые (акустические) для блокировки остеклённых конструкций (Рисунок 7).

Извещатели охранные поверхностные звуковые (акустические) предназначены для обнаружения разрушения остеклённых конструкций в помещениях.

Дальность действия определяется расстоянием от извещателя до наиболее удалённой точки поверхности контролируемого стекла.

Минимальная охраняемая площадь представляет собой минимально допустимую для конкретного типа извещателя площадь поверхности охраняемого им стекла. Как правило, значение минимальной охраняемой площади устанавливают в диапазоне от 0,05 до 0,1 м^2.

Если в охраняемой конструкции установлены стёкла меньших размеров, то необходимо использовать извещатели другого принципа действия, например, ударно-контактные.



Рисунок 7. Извещатели охранные поверхностные звуковые (акустические) для блокировки остеклённых конструкций.

Не следует применять извещатели для блокировки стёкол, имеющих:

- толщину, не соответствующую диапазону, указанному в сопроводительной документации на извещатель;
- линейные размеры, не соответствующие требованиям к минимальной охраняемой площади, указанной в сопроводительной документации на извещатель;
- видимые повреждения (царапины, трещины, сколы и т.п.), снижающие прочность конструкции;
- некачественное (слабое, неплотное, ненадёжное) закрепление стекла в строительной конструкции (раме).

Для обеспечения надёжного обнаружения необходимо при установке извещателя ориентировать его зону обнаружения на блокируемые стёкла.

Для исключения ложных срабатываний от акустических помех извещатель не рекомендуется устанавливать в помещениях:

- с высоким уровнем звуковых шумов (более 65 дБ, что ориентировочно соответствует громкому разговору двух людей в помещении на удалении 3–4 м от извещателя);
- с плохой звукоизоляцией.

В помещении, на период его охраны, должны быть закрыты двери, форточки, отключены вентиляторы, радиоприёмники (или трансляционные громкоговорители) и другие возможные источники звуковых помех.

3.3.2.5 Вибрационные извещатели для блокировки строительных конструкций и сейфов (Рисунок 8).

Вибрационные извещатели предназначены для обнаружения на ранней стадии попытки умышленного разрушения, повреждения или взлома различных строительных конструкций (стены, перекрытия, двери и т.д.), металлических сейфов (шкафов).

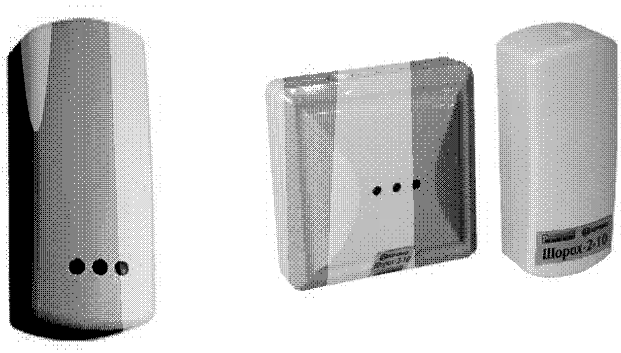


Рисунок 8. Вибрационные извещатели для блокировки строительных конструкций и сейфов (металлических шкафов).

Принцип действия вибрационных извещателей основан на анализе вибрационных сигналов, возникающих в строительных конструкциях при нанесении разрушающих воздействий с целью проникновения в охраняемое помещение.

С помощью таких извещателей можно защитить от вандализма лицевые панели банкоматов, организовать охрану конструкций, выполненных с применением многослойных защитных стёкол и стеклоблоков, кирпичных стен и перегородок, стальных решёток, деревянных дверей, оконных рам (при небольшом размере многосекционных остеклённых проёмов), перекрытий, конструкций из фанеры и древесностружечных плит.

Зона обнаружения вибрационного извещателя может охватывать смежные части сооружения, например, часть пола, потолка, примыкающей стены или капитальной перегородки, если угловое соединение жестко состыковано. В этих случаях дальность действия извещателя для смежных конструкций уменьшается приблизительно на 25 % от установленного значения (новое значение радиуса действия определяется опытным путём).

Охрана строительной конструкции может производиться посредством установки на ней одного или нескольких однопозиционных извещателей или нескольких датчиков вибрации многопозиционного извещателя.

Вибрационный многопозиционный извещатель состоит из блока обработки сигналов (БОС) и комплекта вибрационных извещателей, устанавливаемых непосредственно на охраняемую конструкцию.

Для охраны небольших конструкций, а также дверей, шкафов, сейфов или банкоматов, если их количество не превышает трёх, рекомендуется использовать однопозиционные извещатели, для охраны больших помещений или большого числа строительных конструкций – многопозиционные.

Извещатели обнаруживают разрушающие воздействия на охраняемые конструкции, производимые средствами взлома различной производительности и физического принципа действия, такими, как:

- ручные режущие инструменты (ручные дрели, пилы, напильники);
- термические режущие инструменты (газорежущее, электродуговое оборудование);
- электрические неударные инструменты (электродрели, дисковые пилы типа «болгарка»);
- электрические вращательные инструменты с ударом (электродрели с перфорацией, перфораторы);
- ручные ударные инструменты (молотки, кувалды, ломы, колуны, кирки);
- электрические ударные инструменты (отбойные молотки).

3.3.2.6 Ультразвуковые извещатели для блокировки объёма помещений (Рисунок 9, 10).

Ультразвуковой извещатель использует принцип активной локации.

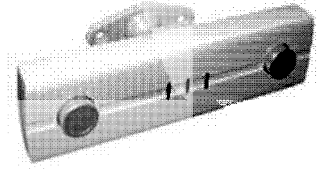


Рисунок 9. Ультразвуковой извещатель для блокировки объема помещения.

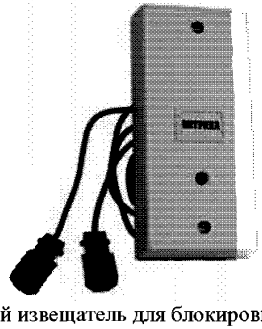


Рисунок 10. Ультразвуковой извещатель для блокировки внутреннего пространства витрин, экспозиций и небольших хранилищ ценностей.

Ультразвуковой извещатель для блокировки объема помещения предназначен для обнаружения движения нарушителя или выявления открытого очага пламени в охраняемой зоне.

При выборе данного извещателя для охраны того или иного объекта необходимо иметь в виду, что акустические волны ультразвукового диапазона, создаваемые извещателем, обладают способностью отражаться от любых твёрдых поверхностей, а также огибать препятствия сравнительно небольших размеров.

Поэтому есть возможность минимизировать образование так называемых «мёртвых зон» (зон нечувствительности).

На функционирование извещателя практически не влияют звуковые помехи, возникающие снаружи охраняемого помещения.

Перемещение мелких домашних животных (грызунов) в зоне обнаружения не вызывает ложных срабатываний извещателя, так как отражающая поверхность этих «нарушителей» (с учётом их малых размеров и наличия шерсти, поглощающей ультразвук) является пренебрежительно малой для извещателя.

Ультразвуковой извещатель для блокировки внутреннего пространства витрин, экспозиций и небольших хранилищ ценностей предназначен для обнаружения проникновения (попытки проникновения) в охраняемую витрину (объём), перемещения предметов в охраняемом объёме.

Извещатель обеспечивает контроль всего объёма охраняемой конструкции путем создания стационарного акустического поля.

3.3.2.7 Оптико-электронные пассивные инфракрасные (ИК) извещатели для блокировки объема помещений и проёмов в строительных конструкциях (Рисунок 11).

Оптико-электронные пассивные ИК извещатели разделяются по типу формируемой зоны обнаружения (ЗО):

- объёмные;
- поверхностные;
- линейные.



Рисунок 11. Извещатели оптико-электронные пассивные ИК.

Они предназначены для обнаружения нарушителя перемещающегося или пересекающего ЗО.

Извещатели, формирующие объёмную ЗО, в свою очередь, подразделяются по способу установки (на стене или на потолке).

Пассивные оптико-электронные ИК извещатели имеют одноблочную конструкцию.

Принцип действия пассивных оптико-электронных ИК извещателей основан на регистрации изменения уровня теплового излучения.

Извещатель рекомендуется устанавливать таким образом, чтобы в его ЗО не попадали потоки тёплого воздуха. В период охраны в помещении должны быть закрыты окна (форточки, фрамуги), балконные и входные двери, отключены обогревательные вентиляторы, кондиционеры и т.п.

Если температура окружающего воздуха ниже (при установке в неотапливаемых помещениях) или выше допустимых значений рабочей температуры извещателя, то извещатель может не обнаруживать нарушителя.

Наличие на входном окне извещателя постоянной или переменной высокой освещённости, фактическое значение которой превышает 6500 лк (ГОСТ Р 50777-14 «Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний»), может являться причиной ложных срабатываний или пропуска нарушителя.

Причиной высокой освещённости может быть как естественные, так и искусственные источники освещения.

Для исключения влияния данного фактора на работу извещателя он должен быть установлен таким образом, чтобы на его входное окно не попадали прямые солнечные лучи и излучение от мощных осветительных приборов.

Следует иметь в виду, что резкое чередование на входном окне извещателя света и тени (вызванное, к примеру, перемещающимися по небу облаками, качающимися ветвями деревьев, перекрывающими солнце и т.п.) негативно влияет на работу извещателя и может являться причиной ложных срабатываний. При этом следует отметить, что сами качающиеся за окном ветки влияния на работоспособность пассивного ИК извещателя, установленного в помещении (при условии, что окна помещения закрыты, что обычно оговаривается в прилагаемой к извещателю эксплуатационной документации), не оказывают.

Оседание на входном окне извещателя твердых мелкодисперсных частиц приводит к уменьшению максимальной рабочей дальности действия и обнаружительной способности извещателя.

При наличии в ЗО крупногабаритных предметов и конструкций (сплошные, сетчатые, стеклянные перегородки), перемещение нарушителя за ними обнаружено не будет.

При этом обеспечить полное отсутствие таких предметов на большинстве объектов невозможно. В этом случае для обеспечения

надёжной охраны необходимо установить несколько извещателей таким образом, чтобы все возможные пути перемещения нарушителя попадали в их ЗО.

Наличие на охраняемом объекте животных, перемещающихся в ЗО извещателя, может привести к ложному извещению о тревоге.

Для охраны таких объектов необходимо применять специальные извещатели, обладающие устойчивостью к перемещению в ЗО животных, а при выборе места их установки и монтаже строго выполнять требования, изложенные в прилагаемой к извещателям эксплуатационной документации.

3.3.2.8 Оптико-электронные активные ИК извещатели для блокировки периметров, конструкций, помещений и отдельных предметов (Рисунок 12, 13).

Линейные оптико-электронные извещатели (активные ИК извещатели) предназначены для обнаружения попыток проникновения на охраняемый объект и формирования извещения о тревоге. В отличие от пассивных ИК извещателей, регистрирующих тепловое излучение нарушителя, активные ИК извещатели регистрируют изменение собственного излучения, вызванное вторжением нарушителя в ЗО.

Достоинством активных ИК извещателей является то, что их обнаружительная способность не зависит от характеристик теплового излучения человека (нарушителя). Также они нечувствительны к изменению характеристик теплового излучения окружающих объектов (фона) и возникающим тепловым помехам.

К недостаткам активных ИК извещателей можно отнести то, что они способны формировать только линейную ЗО, что ограничивает их область применения. Отчасти эта проблема может быть решена путём организации поверхностной ЗО (так называемого ИК барьера) за счет применения извещателей, формирующих несколько ИК лучей, или построения ИК барьера из нескольких извещателей. Но при этом размеры ЗО для первого варианта будут небольшими, а второй вариант потребует увеличения финансовых затрат. К недостаткам можно отнести и их чувствительность к оптическим засветкам.

Активные ИК извещатели, как правило, имеют двухблочную конструкцию (Рисунок 12) и состоят из блока излучателя (БИ) и блока фотоприёмника (БФ), образующих оптическую систему.

Появление в ЗО извещателя оптически непрозрачного объекта вызывает прерывание (или снижение мощности) ИК луча, попадающего в приёмник, который анализирует величину и длительность этого прерывания в соответствии с заданным алгоритмом, формирует извещение о тревоге путём изменения сопротивления контактов, подключаемых к шлейфу сигнализации.



Рисунок 12. Активные линейные двухблочные ИК извещатели.

Извещатели, имеющие одноблочную конструкцию (Рисунок 13), состоят из излучателя и фотоприёмника, объединённых в одном корпусе, и светоотражателя (катафота).

Активными ИК извещателями удобно блокировать проёмы ворот, имеющихся в здании (например, ворота боксов или гаражей для хранения автотранспорта). Помимо прохода человека через проём, извещатель будет обнаруживать и проезд транспортного средства. Если ворота имеют распашную конструкцию и их створки открываются наружу, извещатель также будет обнаруживать факт открытия ворот.



Рисунок 13. Активный линейный одноблочный (с катафотом) ИК извещатель.

Блокировка окон, световых фонарей ИК извещателями установленными снаружи здания, применяется для обнаружения проникновения в здание через проём, и для обнаружения попыток несанкционированного воздействия на оконные конструкции (нередки случаи попыток проникновения в здание через оконный проём путём вынимания стекла без его разрушения, при котором акустические извещатели, установленные в здании, извещение о тревоге не формируют).

3.3.2.9 Радиоволновые извещатели для блокировки объема помещений (Рисунок 14).



Рисунок 14. Радиоволновые извещатели для блокировки объема помещений.

В основе принципа действия радиоволновых извещателей лежит эффект Доплера. При отражении сверхвысокочастотного (СВЧ) радиосигнала от движущегося объекта его частота изменяется.

По конструкции извещатели, как правило, имеют одноблочную схему, в которой содержатся два основных узла: СВЧ модуль, который излучает и принимает сверхвысокочастотные колебания, и процессор, который по определённому алгоритму анализирует параметры доплеровского сигнала, поступающего со смесителя, и принимает решение о формировании извещения о тревоге.

При работе извещателя создаётся объёмная зона обнаружения. Электромагнитное излучение распространяется в объёме помещения и ограничивается его капитальными конструкциями.

Вместе с тем, излучение может проникать в соседнее помещение через перегородки, изготовленные на основе древесностружечных плит, фанеры, гипсокартона и т.д., через деревянные и пластмассовые двери, на улицу – через оконные проёмы. В этом случае движение людей, крупных животных, автомобилей за габаритами помещения может привести к формированию ложной тревоги.

Радиоволновые извещатели, предназначенные для блокировки объема помещений, сохраняют работоспособность в широком диапазоне температур, не реагируют на световые засветки, тепловые потоки и сквозняки, имеют стабильную объёмную зону обнаружения, допускают маскировку радиопрозрачными материалами.

Извещатели могут формировать ложные тревоги от вибрации крупных предметов, люминесцентного освещения, перемещения людей или механизмов за оконными проёмами или тонкими перегородками.

3.3.2.10 Комбинированные извещатели для блокировки объема помещений (Рисунок 15, 16).



Рисунок 15. Комбинированный (СВЧ + ИК) извещатель для блокировки объема помещения (устанавливается на стене).



Рисунок 16. Комбинированный (СВЧ + ИК) извещатель для блокировки объема помещения (устанавливается на потолке).

Рекомендуемая область применения комбинированных (СВЧ + ИК) извещателей – блокировка объема помещений с повышенным уровнем помех, мест сосредоточения ценностей, музейных экспонатов, оргтехники, а также помещений критически важных объектов.

В извещателях этого класса используются два физических принципа обнаружения движущегося объекта: регистрация изменения теплового фона, возникающего при пересечении чувствительных зон, формируемых оптической системой, и регистрация наличия доплеровской составляющей в спектре отражённого сигнала, создаваемого СВЧ модулем. При появлении нарушителя в зоне обнаружения срабатывают оба канала (в любой последовательности, с разнесением по времени), формируется извещение о тревоге.

Комбинированные извещатели обладают повышенной помехоустойчивостью по сравнению с собственно радиоволновыми или

пассивными ИК извещателями, так как вероятность возникновения в помещении помех, одновременно воздействующих на два канала, достаточна мала.

Комбинированные (СВЧ + ИК) извещатели надёжно работают в помещениях с повышенным уровнем помех, в которых радиоволновые или оптико-электронные пассивные извещатели, функционирующие по отдельности, выдают ложные извещения о тревоге.

3.3.2.11 Комбинированные (ультразвуковые + ИК) извещатели для блокировки объема помещений (Рисунок 17).

Основная область применения комбинированных (ультразвуковых + ИК) извещателей – помещения, имеющие следующие особенности:

- со сложной помеховой обстановкой внутри и снаружи помещения;
- с остеклёнными (оконными, дверными) конструкциями, выходящими на оживлённую улицу, в том числе остеклённые вестибюли зданий, бизнес-центров, магазинов, выставочных павильонов;
- имеющие некапитальные стены или перегородки со смежными помещениями, где возможно нахождение людей в период охраны.

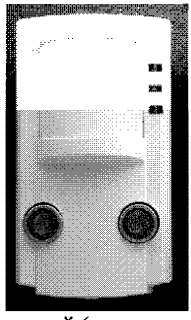


Рисунок 17. Комбинированный (ультразвуковой + ИК) извещатель для блокировки объема помещений.

Принцип работы комбинированных (ультразвуковых + ИК) извещателей заключается в комбинировании двух принципов обнаружения стандартной цели (человека) в охраняемом помещении.

Первый принцип заключается в регистрации ИК излучения при пересечении человеком элементарных зон обнаружения, формируемых оптической системой ИК канала извещателя.

Второй принцип работы извещателя основан на эффекте Доплера, в соответствии с которым частота ультразвукового сигнала, отражённого от движущегося препятствия, отличается от первоначальной на величину, которая прямо пропорциональна излучаемой частоте и радиальной скорости движения отражателя и обратно пропорциональна скорости распространения ультразвука в контролируемой среде.

Следует отметить, что размеры зоны можно изменять так, как нужно в конкретных условиях (габаритах помещения), в том числе для создания локального охраняемого пространства.

3.3.2.12 Совмещённые извещатели для блокировки объема помещений и остеклённых конструкций (Рисунок 18).

Область применения совмещённых (ИК + акустический) извещателей – помещения с остеклёнными (оконными, дверными) конструкциями.

Извещатели сочетают в себе два принципа обнаружения (ИК + акустический), обнаруживают движение нарушителя в закрытом охраняемом помещении и разрушение строительных конструкций, выполненных с использованием листового стекла (обычного, армированного, узорчатого, закалённого, трёхслойного, ударостойкого), стеклоблоков, однокамерных и двухкамерных стеклопакетов.



Рисунок 18. Совмещённые извещатели для блокировки объема помещений и остеклённых конструкций.

При появлении человека в зоне обнаружения срабатывает ИК канал обнаружения, при разбитии стекла – акустический канал (в любой последовательности или одновременно). При этом выдаётся извещение о тревоге путем размыкания контактов соответствующего выходного реле.

3.3.2.13 Извещатели для тревожной сигнализации (ТС) о нападении (тревожные кнопки, педали и т.п.).

Для оперативной передачи сообщений в дежурную часть органов внутренних дел или на ПЦН о нападении нарушителя объект оборудуют техническими средствами ТС.

Извещатель (Рисунок 19) представляет собой тревожную кнопку для выдачи извещения о нападении с фиксацией извещения. Перевод извещателя в дежурный режим после нажатия кнопки осуществляется при помощи ключа, который хранится в подразделении охраны.



Рисунок 19. Тревожная кнопка с фиксацией.

Извещатель (Рисунок 20) предназначен для подачи сигнала тревоги ногой при нападении преступников на сотрудников.

Система ТС должна быть выполнена «без права отключения», выведена на пульт внутренней охраны, на ПЦН.



Рисунок 20. Тревожный извещатель для подачи сигнала тревоги ногой при нападении преступников.

3.4 Критерии выбора СОТС.

Критерии выбора СОТС:

- назначение и функции, выполняемые техническими средствами охранной сигнализации;
- вид предполагаемой угрозы объекту;
- помехозащищённость;
- надёжность;
- круглосуточный режим функционирования;
- функционирование в автоматическом режиме;
- функционирование в автономном режиме;
- самодиагностирование;
- бесперебойное электропитание;
- возможность расширения как функциональных, так и количественных характеристик системы;
- интеграция в единую систему безопасности;

- защита информации от несанкционированного внешнего доступа и копирования при передаче от периферийных узлов на пульт дежурного;
- соответствие российским и международным стандартам.

3.5 Организация передачи информации на пульт централизованного наблюдения.

3.5.1 Передача извещений о срабатывании охранной сигнализации (ОС) с объекта на ПЦН может осуществляться с ППК, внутреннего пульта охраны или УОО СПИ.

3.5.2 Количество рубежей ОС, выводимых на ПЦН отдельными условными номерами, определяется совместным решением руководителя объекта и подразделения вневедомственной охраны исходя из категории объекта, анализа риска и потенциальных угроз объекту, возможностей интеграции и документирования ППК (внутренним пультом охраны или УОО СПИ) поступающей информации, а также порядком организации дежурства на объекте.

3.5.3 При наличии на объекте пульта внутренней охраны с круглосуточным дежурством, на ПЦН выводятся:

- один общий сигнал, объединяющий все рубежи ОС объекта, за исключением рубежей специальных помещений объекта;
- рубежи ОС (периметр и объём) специальных помещений.

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

3.5.4 При наличии на объекте пульта внутренней охраны с круглосуточным дежурством сотрудников подразделений вневедомственной охраны (Микро–ПЦН), все рубежи ОС помещений объекта (включая и специальные помещения) подключаются на пульт внутренней охраны, обеспечивающий автоматическую регистрацию всей поступающей информации, а с него выводится один общий сигнал на ПЦН.

На объектах, где охраняются только специальные помещения, выводу на ПЦН подлежат все рубежи ОС этих помещений.

3.5.5 Рубежи ОС должны выводиться на ПЦН с пульта внутренней охраны, ППК или УОО СПИ, обеспечивающих запоминание тревожного состояния и его фиксацию на выносном световом (звуковом) оповещателе или индикаторе.

Извещения от шлейфов ОС одним объединенным сигналом выводятся на ПЦН и в дежурную часть органов внутренних дел Российской Федерации непосредственно или через ППК, УОО СПИ, пульт внутренней охраны.

3.5.6 Для исключения доступа посторонних лиц к извещателям, ППК, разветвительным коробкам, другой установленной на объекте аппаратуре охраны должны приниматься меры по их маскировке и скрытой установке. Крышки клеммных колодок данных устройств должны быть опломбированы

(опечатаны) электромонтёром охранно-пожарной сигнализации или инженерно-техническим работником подразделения вневедомственной охраны с указанием фамилии и даты в технической документации объекта.

3.5.7 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 ПЦН в составе ТС.

3.5.8 Извещения СОТС могут передаваться на ПЦН 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 с обязательным контролем канала между охраняемым объектом и ПЦН.

Проводная среда передачи информации реализуется в виде:

- абонентской телефонной сети общего пользования или специально прокладываемой выделенной линии оператора связи (технология DSL, FTTC, FTTB, в т.ч. по технологии GPON);
- линии связи интернет провайдеров (коаксиальный кабель, «витая пара», оптоволоконный кабель);

Беспроводная среда передачи информации может быть реализована в виде:

- выделенных рабочих частот УКВ радиодиапазона;
- защищённых каналов передачи данных сетей сотовых операторов стандарта GSM(GPRS) - VPN.

3.6 Электропитание.

СОТС, согласно Р 78.36.032-2013 (п.9) и ПУЭ (п.1.2.17.), относится к 1 категории электроприёмников по надёжности электроснабжения, в силу чего электропитание должно быть бесперебойным.

При пропадании основного электропитания 220В, 50 Гц СОТС автоматически переходит на электропитание от резервного источника электропитания (аккумулятора) постоянного напряжения 12В без выдачи сигналов тревоги, но с формированием служебного сообщения «переход на резервное электропитание».

При переходе на электропитание от резервного источника электропитания (аккумулятора) должна обеспечиваться бесперебойная работа оборудования и извещателей СОТС не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги.

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

- в городах и поселках городского типа - до 4 часов в дежурном режиме и до 1 часа в режиме тревоги;
- 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.

Пример расчёта резервного источника электропитания при наличии автоматического или иного оповещения подразделения вневедомственной охраны о моменте отключения основного электропитания в городах и поселках городского типа - до 4 часов в дежурном режиме и до 1 часа в режиме тревоги.

№	Наименование	Кол-во, шт.	Ток потребления одним устройством в дежурном режиме, мА	Ток потребления одним устройством в режиме тревоги, мА	Суммарный ток потребления в дежурном режиме, мА	Суммарный ток потребления, в режиме тревоги, мА
1	Пульт контроля и управления охранно-пожарный	1	60	120	60	120
2	Прибор приёмно-контрольный ёмкостью на 20 шлейфов	2	600	650	1200	1300
3	Релейный модуль	1	300	300	300	300
4	Пульт непрограммируемый	1	60	120	60	120
5	Устройство оконечное объектовое СПИ	1	150	250	150	250
6	Извещатель охранный объёмный радиоволновый	4	25	25	100	100
7	Извещатель охранный объёмный оптико-электронный	10	20	20	200	200
8	Извещатель	8	20	20	160	160

	охранный поверхностный оптико-электронный					
9	Извещатель охранный поверхностный звуковой	10	20	20	200	200
10	Радиоприёмник	1	80	80	80	80
	ИТОГО				2510	2830

Необходимая ёмкость аккумулятора рассчитывается по формуле:

Q(мАч) = 1,2 х Iр(мА) х t(ч),

где:

1,2 - коэффициент запаса ёмкости;

Iр - потребляемый ток (мА);

t - требуемое время работы (ч).

Необходимая ёмкость аккумулятора в дежурном режиме составляет:

1,2 х 2510 мА х 4 ч =12488 мАч.

Необходимая ёмкость аккумулятора в режиме тревоги составляет:

1,2 х 2830 мА х 1 ч = 3396 мАч.

12488 мАч.+ 3396 мАч.=15884 мАч.

Согласно расчётам выбираем резервированный источник электропитания, удовлетворяющий следующим характеристикам:

- максимальный ток нагрузки не менее 2,83 А;
- ёмкость аккумулятора должна быть не менее 15,884 Ач.

Заземление оборудования и устройств должно выполняться в соответствии с требованиями СНиП 3.05.06-85, ПУЭ, технической документации предприятий-изготовителей.

3.7 Общие требования к минимально необходимому составу СОТС.

3.7.1 Требования к защите СОТС зданий, помещений, отдельных предметов.

ТСО должны оборудоваться все помещения с постоянным или временным хранением материальных ценностей, а также все уязвимые места здания (окна, двери, люки, вентиляционные шахты, короба и другие проёмы), через которые возможно несанкционированное проникновение в помещения объекта.

Для защиты вентиляционных шахт, коробов и дымоходов сечением более 200 мм, имеющих выход за границы охраняемой территории объекта, в том числе на крыши зданий, а также в смежные неохраняемые помещения и своим сечением входящие в охраняемые помещения, допускается использование фальшрешёток с ячейкой 100 х 100 мм, выполненных из

металлических трубок с диаметром отверстия не менее 6 мм для протяжки провода шлейфа сигнализации «на обрыв», а также применение иных ТСО.

В случае наличия на охраняемых объектах неиспользуемых подвальных помещений необходимо, при отсутствии двери на выходе из них, установить металлическую открывающуюся решётчатую дверь, закрывающуюся на навесной замок, и оснастить её ТСО.

Ключи от замков на оконных решётках и дверях запасных выходов должны быть размещены в непосредственной близости или в специально выделенном помещении (в помещении охраны) в ящике, шкафу или нише, заблокированных ОС.

Устанавливаемые ТСО СОТС должны вписываться в интерьер помещения и по возможности устанавливаться скрытно.

В разных рубежах ОС необходимо применять охранные извещатели, работающие на различных физических принципах действия.

Количество шлейфов ОС должно определяться тактикой охраны, размерами зданий, строений, сооружений, этажностью, количеством уязвимых мест, а также точностью определения места проникновения для быстрого реагирования на извещения о тревоге.

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

Для усиления охраны и повышения её надежности на объектах следует устанавливать дополнительные извещатели-ловушки. Сигналы ловушек выводятся по самостоятельным или, при отсутствии технической возможности, по имеющимся шлейфам ОС.

В помещениях, где круглосуточно должны находиться сотрудники полиции, ОС должны оборудоваться отдельные участки периметра помещения, а также сейфы и металлические шкафы для хранения ценностей и документов.

Помещения объектов оборудуются многорубежной системой ОС, а вспомогательные помещения – однорубежной.

3.7.2 Охранная сигнализация.

ОС оборудуются:

- периметр зданий (помещений) и сооружений (оконные проемы, двери, люки, ворота и другие) с выводом на внутренний пост охраны (дежурная часть);
- отдельные служебные помещения с выводом на внутренний пост охраны (дежурную часть);
- специальные помещения с выводом на внутренний пост охраны (дежурную часть) и ПЦН.

Первым рубежом ОС, в зависимости от вида предполагаемых угроз объекту, блокируют:

- входные двери, погрузочно-разгрузочные люки, ворота – на «открывание», «разрушение» и «пролом»;
- деревянные, стеклянные и остеклённые конструкции – на «открывание», «разрушение» и «разбитие» стекла;
- стены, перекрытия и перегородки, за которыми размещаются помещения других собственников – на «разрушение» и «пролом»;
- вентиляционные короба, дымоходы, места ввода/вывода коммуникаций сечением более 200 х 200 мм – на «разрушение» и «пролом».

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

Вторым рубежом ОС защищаются объемы помещений на «проникновение» с помощью объёмных извещателей различного принципа действия.

Третьим рубежом ОС в помещениях блокируются отдельные предметы, сейфы, металлические шкафы, в которых сосредоточены документы и ценности.

Специальные помещения.

Комната хранения оружия (КХО).

КХО должна быть оборудована не менее, чем двумя рубежами охранной сигнализации.

Первым рубежом охраны блокируются:

1. Входная дверь – на открывание и пролом (разрушение).

2. Окно для выдачи оружия и боеприпасов – на открывание и пролом (разрушение).

3. Наружные стены КХО (наружные стены здания) – на пролом (разрушение).

Вторым рубежом ОС блокируется объём помещения.

Третьим рубежом охранной сигнализации блокируется металлический шкаф (сейф) – на открывание и пролом (разрушение).

Специальные помещения: для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, архивы, хранилища, кассы и другие защищаются в два рубежа охраны.

Первым рубежом ОС блокируются:

1. Входные двери в помещения – на открывание;

2. Окна – на открывание и разбитие.

Вторым рубежом ОС – объём помещения.

Дополнительным рубежом ОС в помещениях могут блокироваться отдельные предметы, сейфы, металлические шкафы, в которых сосредоточены документы и ценности.

Для блокировки помещений двумя (тремя) рубежами охраны применяются охранные извещатели, работающие на различных физических принципах действия.

Сигнализация из КХО и комнаты для хранения средств защиты, связи, специальной, оперативной и криминалистической техники должна быть выведена на ПЦН ближайшего подразделения вневедомственной охраны и непосредственно на рабочее место оперативного дежурного.

3.7.3 Тревожная сигнализация.

Для передачи тревожных извещений в дежурную часть о противоправных действиях в отношении сотрудников и работников (угроз террористического и криминального характера) объект оборудуется устройствами ТС.

Устройства тревожной сигнализации на объекте должны устанавливаться:

- в специальных помещениях (дежурных частей, комнатах хранения оружия, боеприпасов и специальных средств, для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, архивах, хранилищах, кассах и других);
- у центрального входа в здание и запасных выходов из него;
- на всех наружных и внутренних постах охраны и в помещении охраны;
- в иных местах, регламентированных правовыми актами МВД России.

Рекомендуется использовать мобильные устройства ТС, работающие по радиоканалу (радиокнопки или радиобрелоки).

Устройства тревожной сигнализации размещаются в местах, по возможности незаметных для посетителей.

Решение о необходимости вывода сигнала на ПЦН принимается руководителем подразделения, в ведении которого находится объект, исходя из его функционального назначения, степени потенциальной опасности, которой он может подвергаться, а также анализа вероятных угроз объекту и характеристики его уязвимости.

Обобщённый сигнал от КТС подключается на ПЦН без права отключения.

Примечания:

1. Аттестованные помещения, а также помещения, предназначенные для обработки сведений, составляющих государственную тайну, оборудуются техническими средствами ОС, прошедшими сертификацию по стандартам ФСТЭК России и ФСБ России.

2. В случае отсутствия (с учетом объективных факторов) на объекте необходимых средств инженерно-технической укреплённости (решётки на окнах и т.д.) либо оснащённости объекта средствами инженерно-технической укреплённости более низкого класса защиты, рекомендуется оборудовать

объект дополнительными рубежами охраны с использованием средств охранной сигнализации и системы охранной телевизионной.

Организация дополнительных рубежей охраны должна быть согласована с подразделением охраны и руководством объекта.

ПРИЛОЖЕНИЯ

Приложение 1

Условные обозначения

Наименование	Обозначение
Пульт управления программируемый	
Прибор приемно-контрольный охранно-пожарный	
Устройство взятия-снятия СПИ	
Устройство оконечное объектовое СПИ	
Релейный блок	
Радиосистема тревожной сигнализации (приемник)	
Извещатель охранный магнитоконтактный для деревянных окон, дверей	
Извещатель охранный магнитоконтактный для металлических дверей	
Извещатель охранный поверхностный оптико-электронный (пассивный ИК)	
Извещатель охранный объемный оптико-электронный (пассивный ИК)	
Извещатель охранный объемный радиоволновый	
Извещатель охранный поверхностный вибрационный	
Извещатель охранный совмещенный вибрационный с датчиком наклона.	
Извещатель охранный поверхностный звуковой (акустический)	
Извещатель охранный омический	
Кнопка тревожной сигнализации	
Кнопка тревожной сигнализации радиоканальная (брелок)	
Оповещатель охранно-пожарный световой	
Оповещатель охранно-пожарный звуковой	
Источник резервированного электропитания 12В	
Бесперебойный источник питания 220В	
Адресная линия связи	
Шлейф сигнализации	

Приложение 2

Схема блокировки двери, окна извещателем охранным магнитоконтактным

Схема блокировки двери

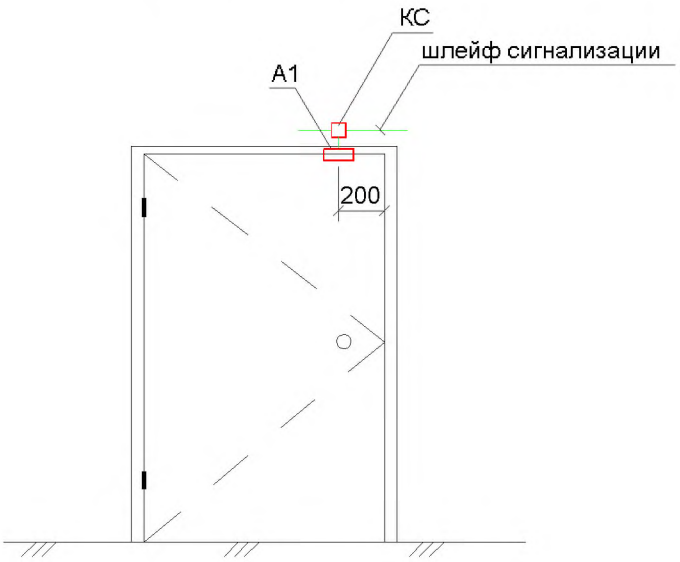
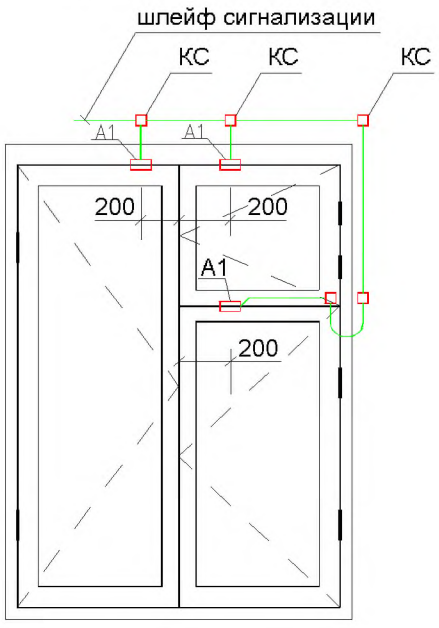


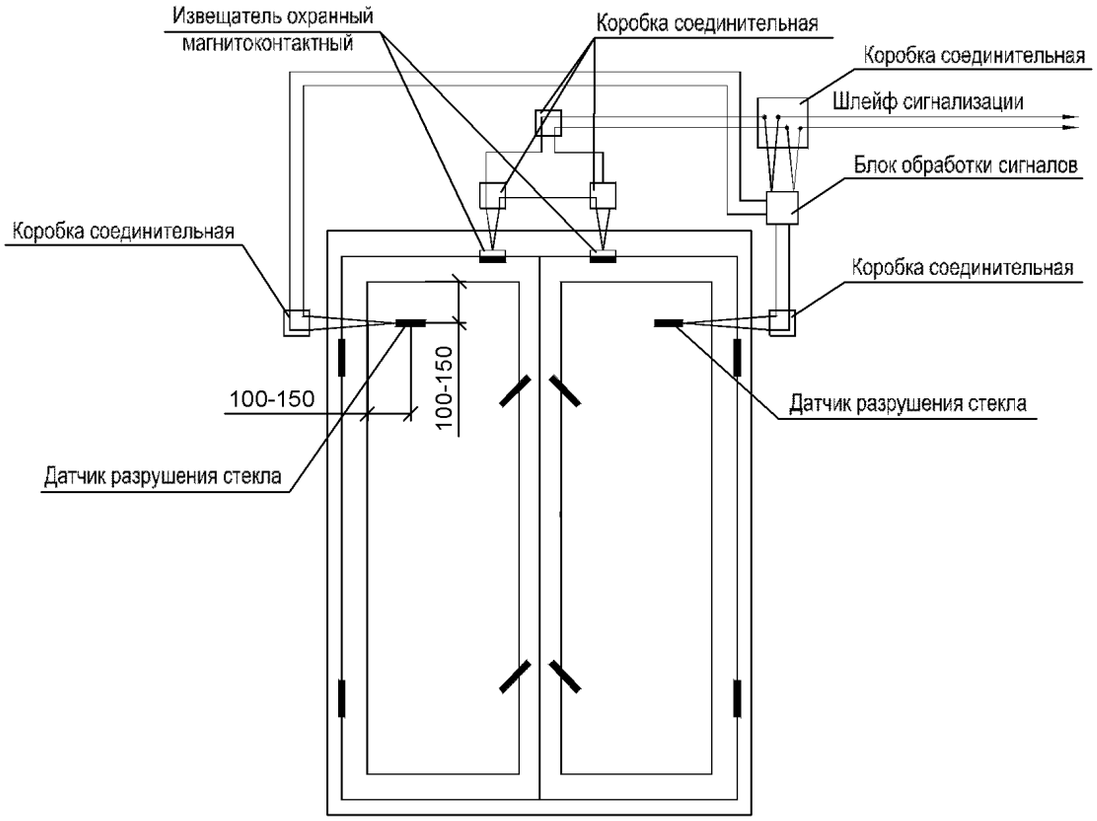
Схема блокировки окна



А1- Извещатель охранный магнитоконтактный
КС- Коробка соединительная

Приложение 3

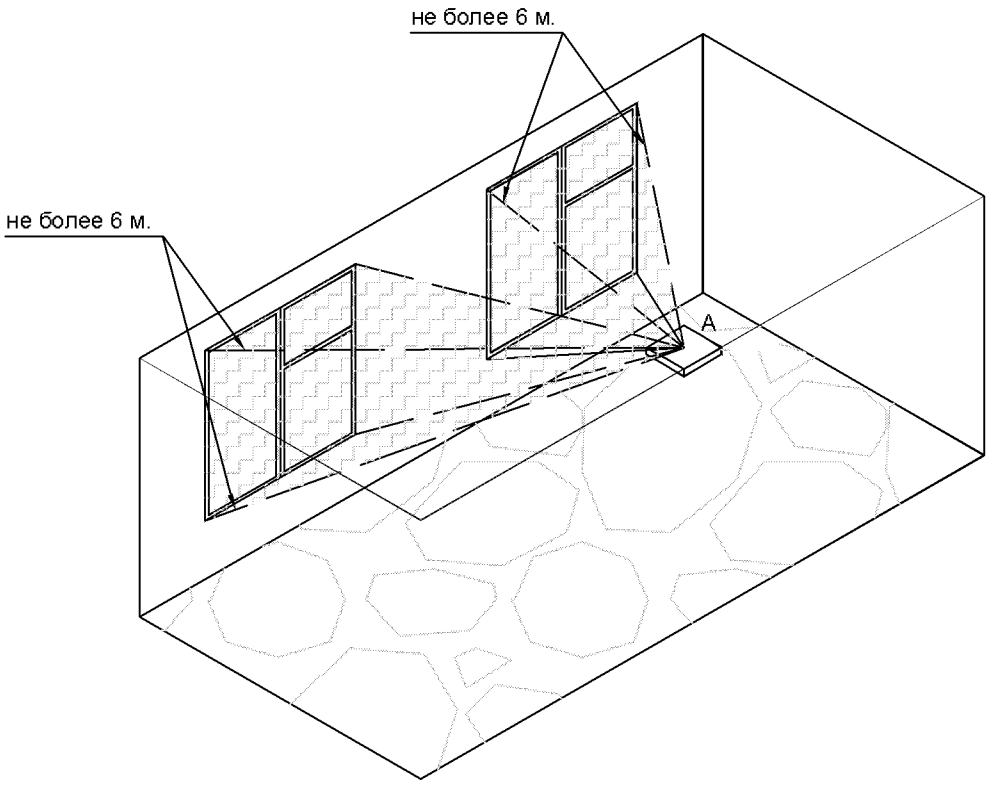
Схема установки извещателя охранного ударно-контактного для блокировки окна



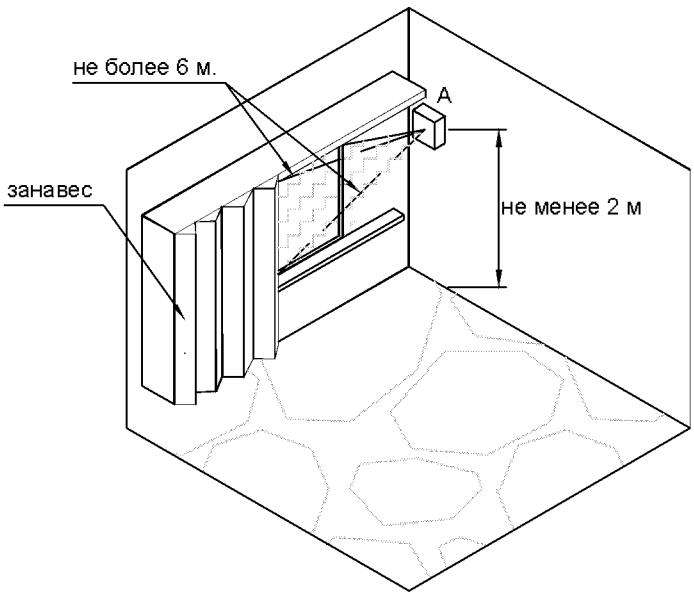
Приложение 4

Схема установки извещателя охранного поверхностного звукового (акустического)

Установка на потолке



Установка извещателя между стеклом и занавесом (жалюзи)



А-Извещатель охранный поверхностной звуковой (акустический)

Приложение 5

Схема установки извещателя охранного поверхностного оптико-электронного (инфракрасного)

Зоны обнаружения

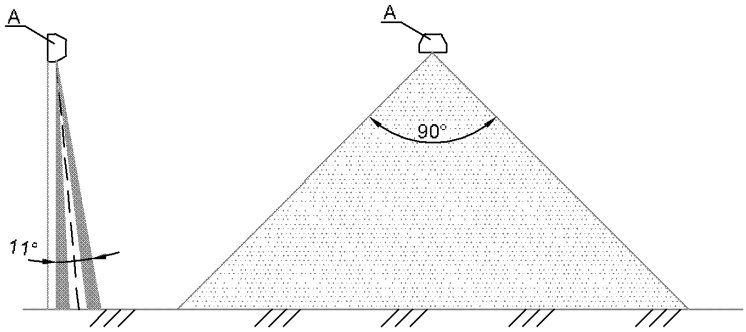
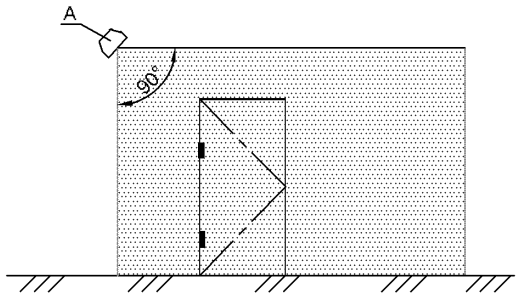


Схема блокировки двери



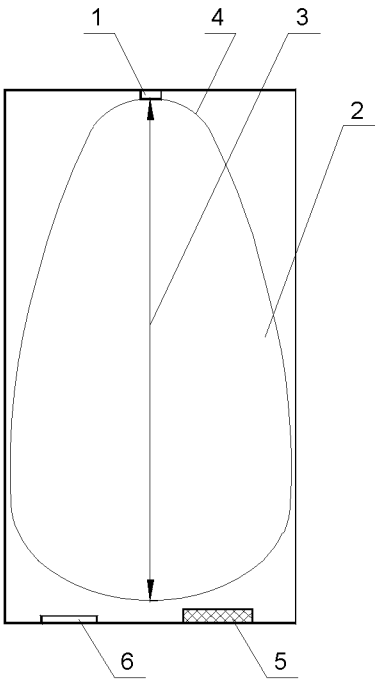
А-Извещатель охранный поверхностной оптико-электронный

Приложение 6

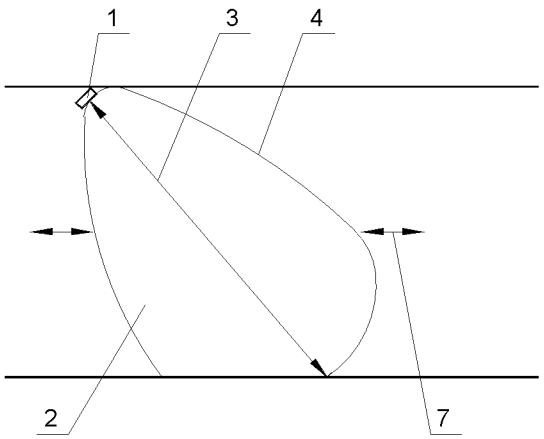
Схема установки извещателя охранного объемного ультразвукового

Вид сверху

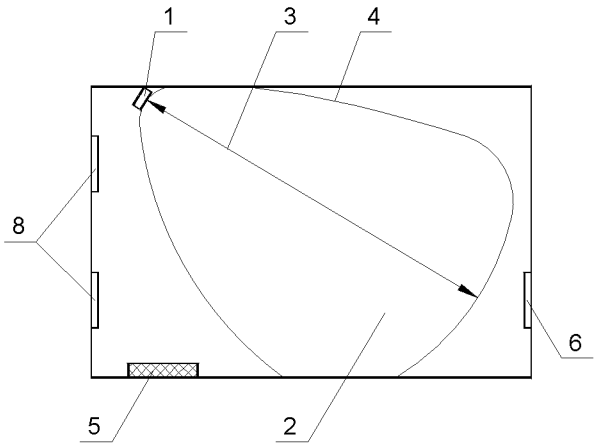
Вариант 1



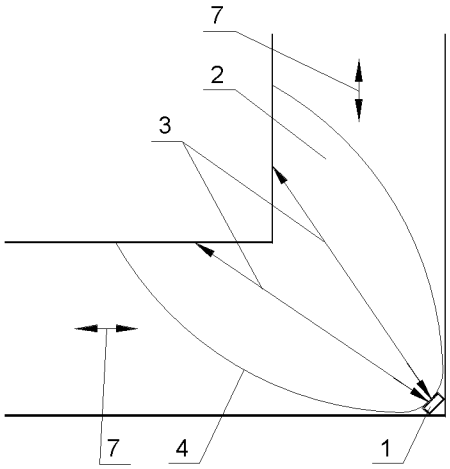
Вариант 2



Вариант 3



Вариант 4

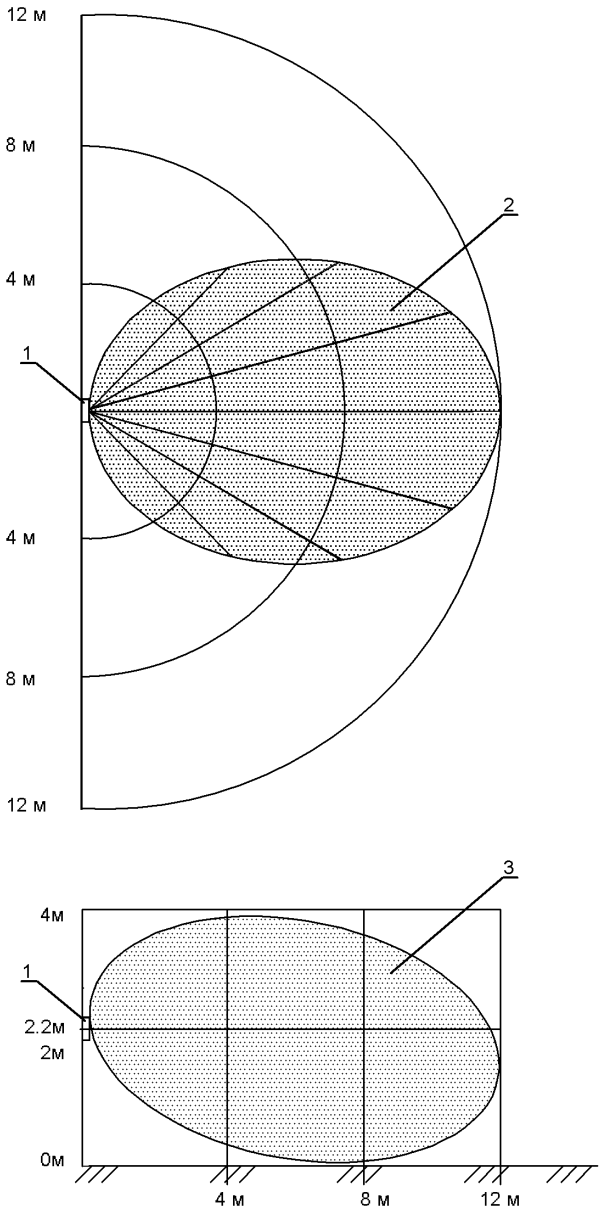


1-извещатель
2-зона обнаружения (ЗО)
3-дальность действия (осевая линия ЗО)
4-граница ЗО
5-электрообогреватель или батарея отопления
6-дверь
7-наиболее вероятное направление движения нарушителя
8-окно

Приложение 7

Схема установки извещателя охранного объемного радиоволнового

Зоны обнаружения



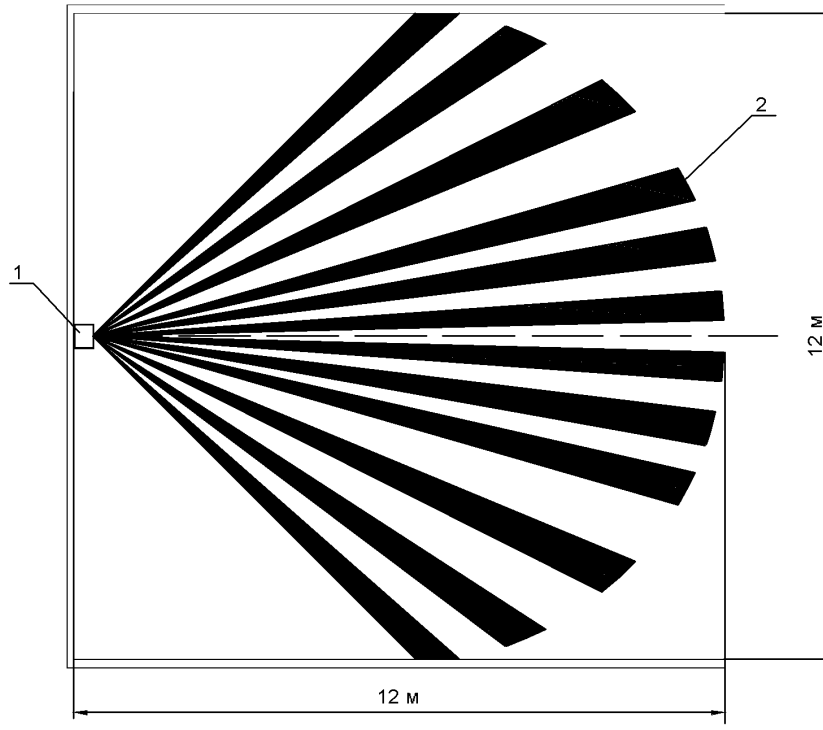
1-Извещатель охранный объемный радиоволновой
2-Зона обнаружения в горизонтальной плоскости
3-Зона обнаружения в вертикальной плоскости

Приложение 8

Схема установки извещателя охранного объемного оптико-электронного (инфракрасного)

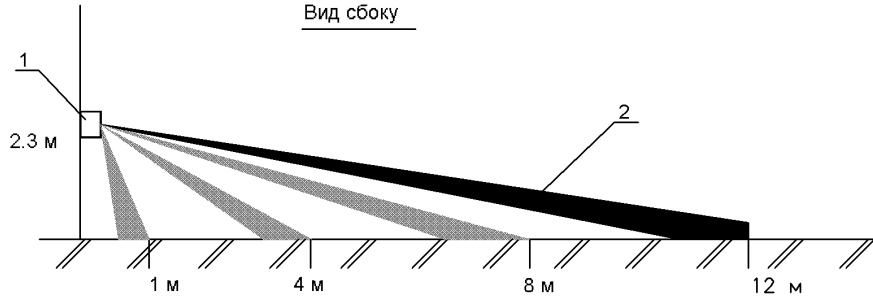
Оптико-электронный канал

Вид сверху



Оптико-электронный канал

Вид сбоку

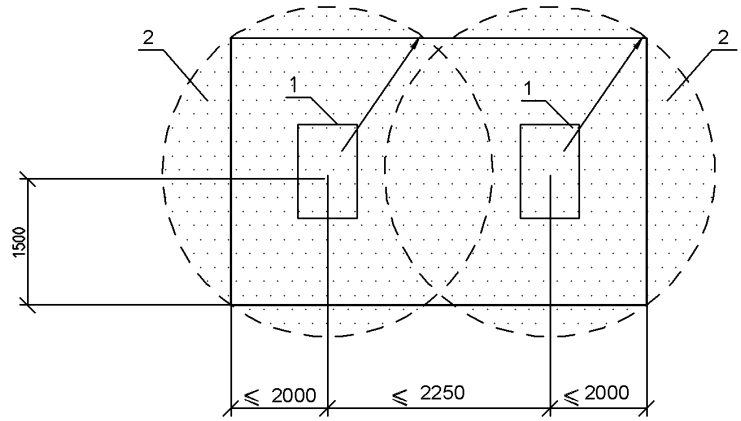


1-Извещатель охранный оптико-электронный (инфракрасный)
2-Зона обнаружения

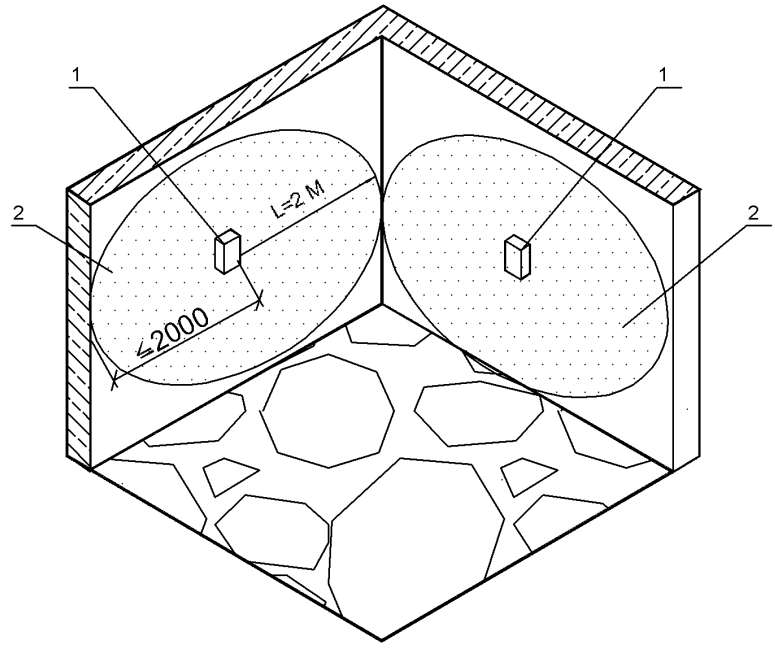
Приложение 9

Схема установки извещателя охранного поверхностного вибрационного на стене

Зоны обнаружения



Полная защита конструкции

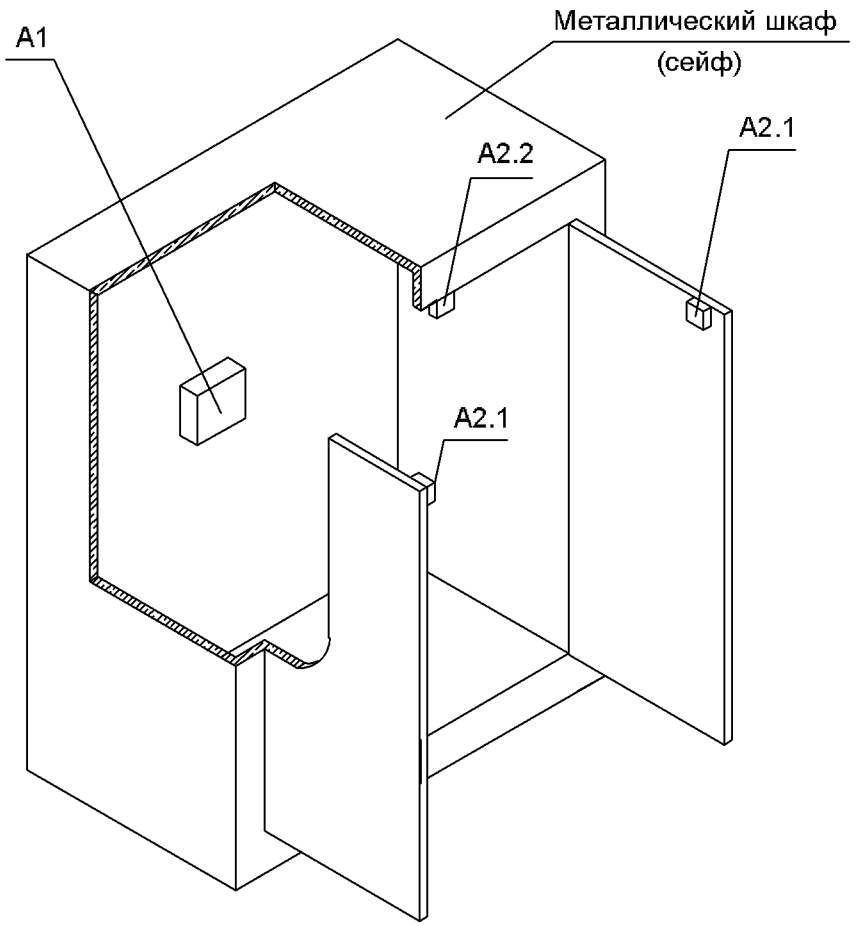


1- Извещатель охранный поверхностный вибрационный.

2- Зона обнаружения

Приложение 10

Схема установки извещателя охранного поверхностного вибрационного с датчиком наклона



A1- Извещатель охранный поверхностный вибрационный с датчиком наклона

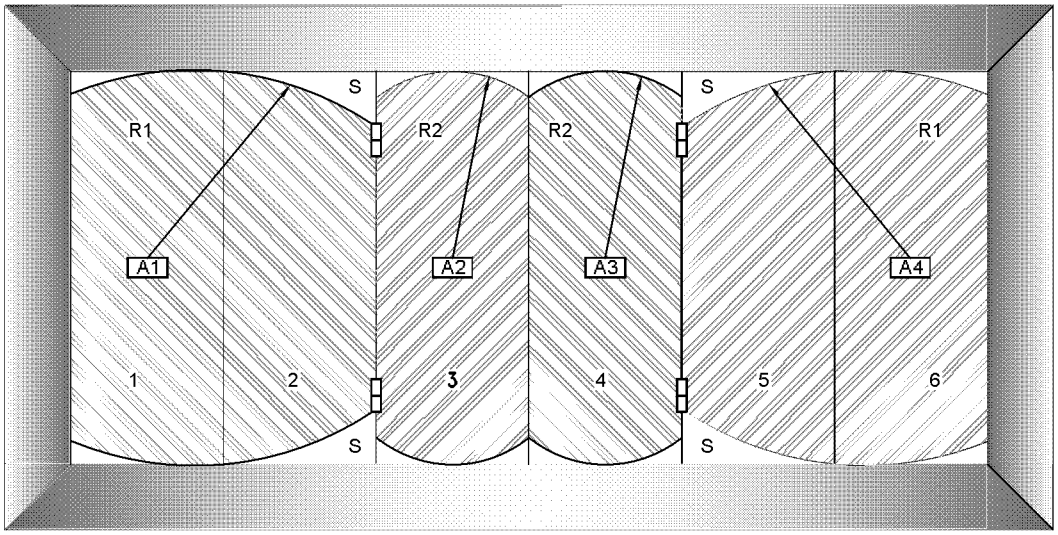
A2.1- Извещатель охранный магнитоконтактный (магнит)

A2.2- Извещатель охранный магнитоконтактный (геркон)

Все охранные извещатели устанавливаются внутри металлического шкафа

Приложение 11

Схема установки извещателя охранного поверхностного вибрационного для охраны немонолитной (многосекционной) конструкции



A1-A4 - многофункциональный вибрационный извещатель

R1- радиус действия для элементов конструкций 1,2 и 5,6, имеющих жесткую связь для передачи вибрации при разрушении

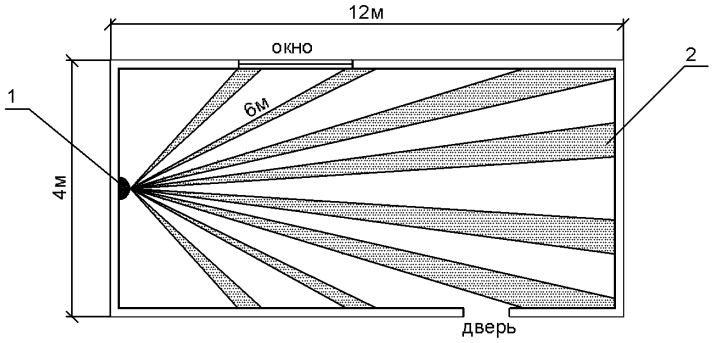
R2- радиус действия для элементов конструкций 3 и 4, не имеющих связи для передачи вибрации при разрушении

S - площадь, не охваченная радиусом R1 или R2($S < 0{,}1 м^2$)

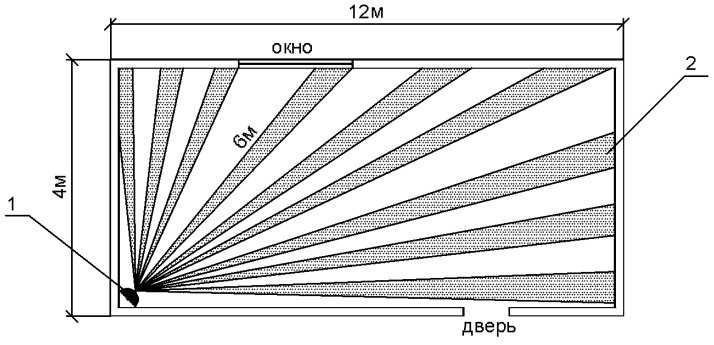
Приложение 12

Схема установки извещателя охранного объемного совмещенного (ИК+АК)

Установка на боковой стене



Установка в углу



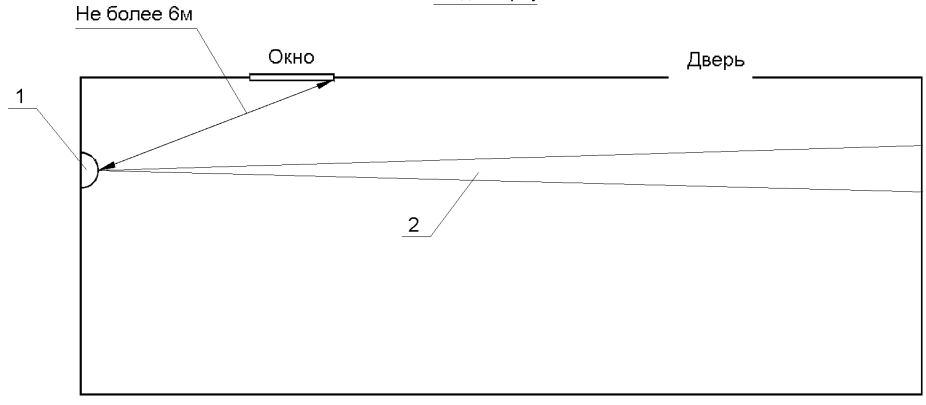
1- Извещатель охранный объемный совмещенный

2- Зона обнаружения

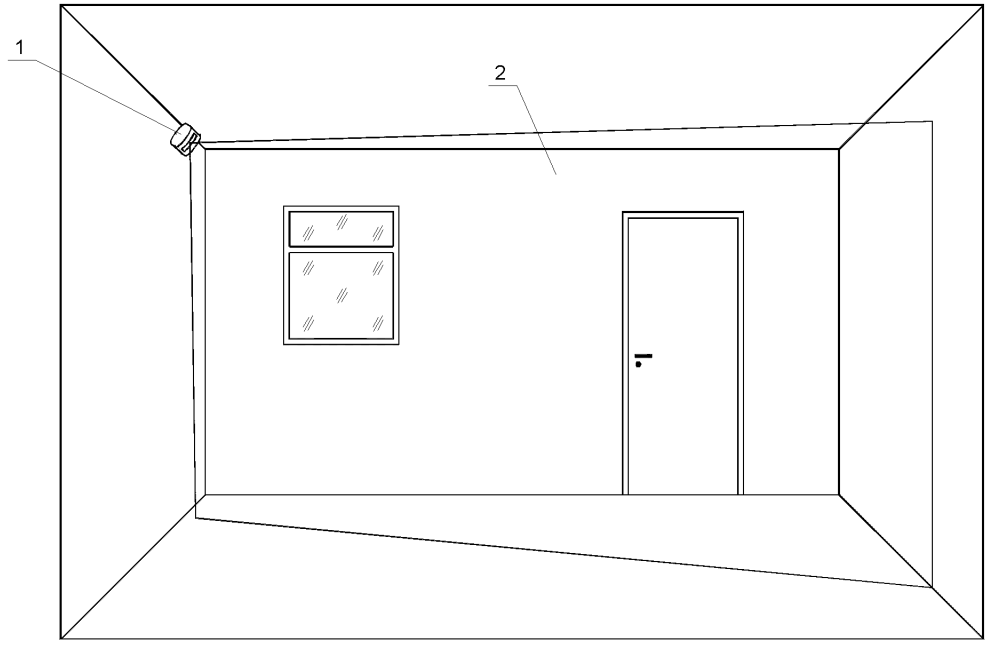
Приложение 13

Схема установки извещателя охранного поверхностного совмещенного (ИК+АК)

Вид сверху



Вид с боку

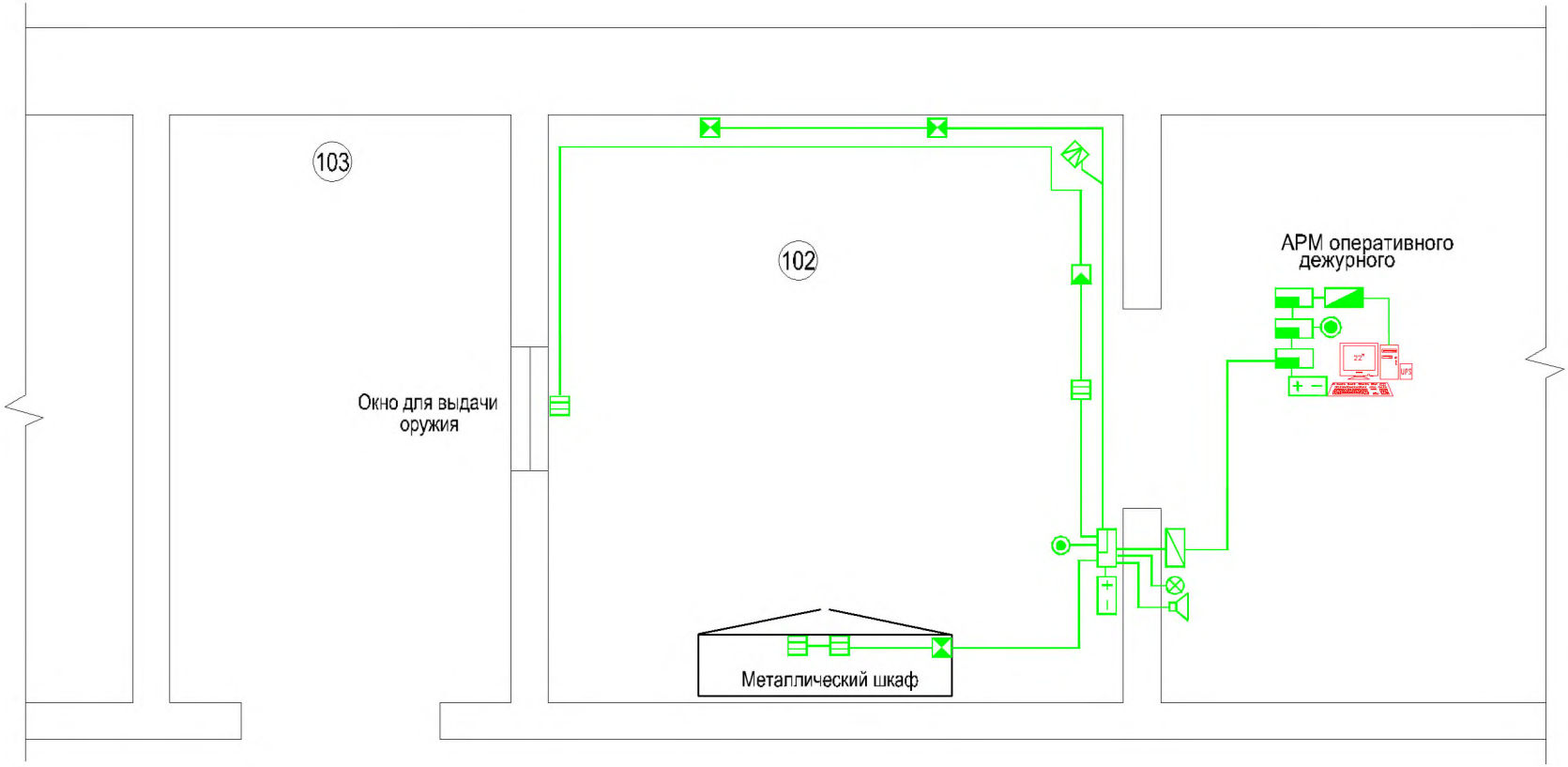


1- Извещатель охранный поверхностный совмещенный (ИК+АК).

2- Зона обнаружения ИК канала.

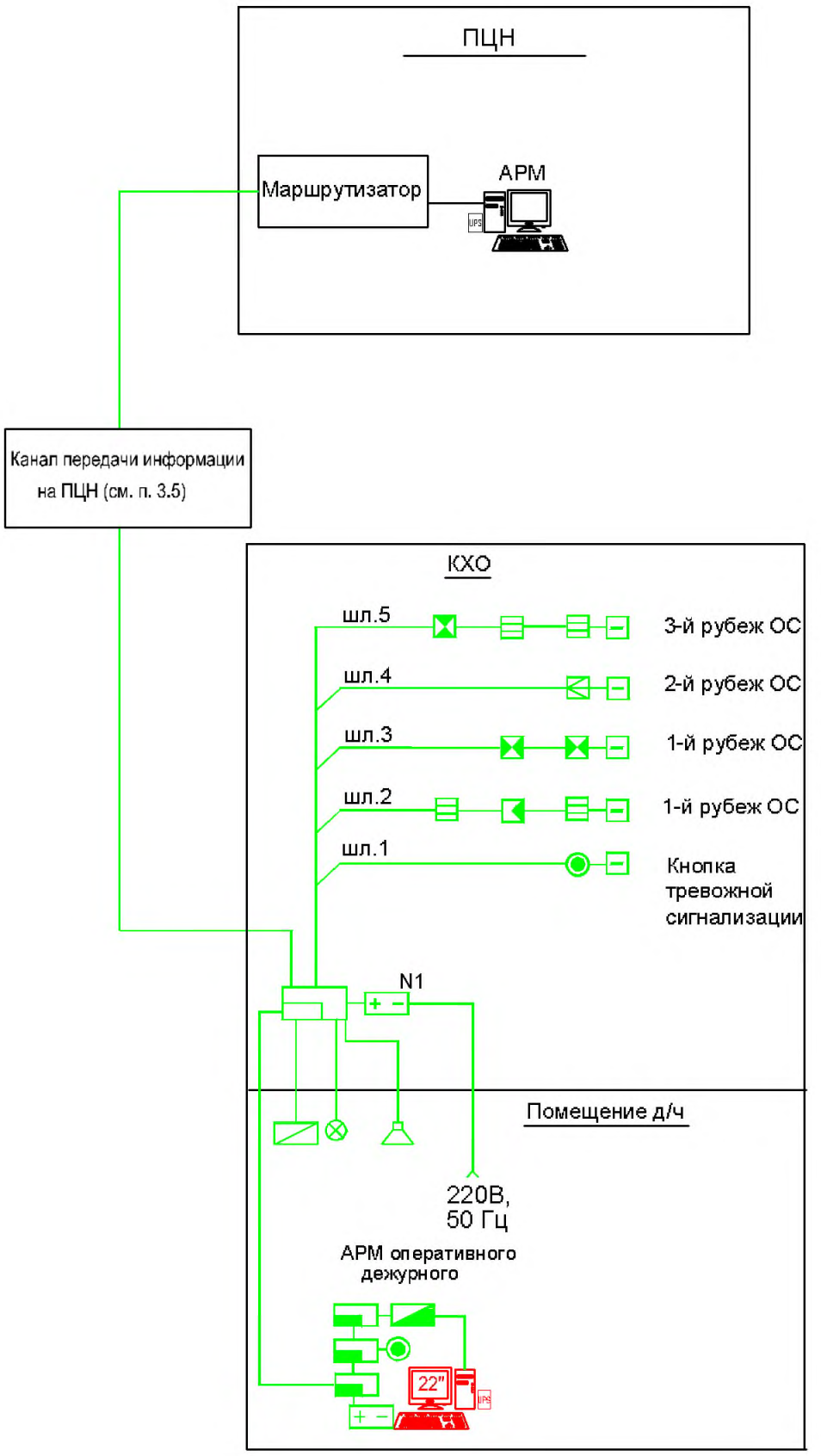
Приложение 14

План расположения оборудования СОТС комнаты хранения оружия



№ п/п	Наименование
102	Комната хранения оружия
103	Комната чистки оружия

Комната хранения оружия. Схема структурная

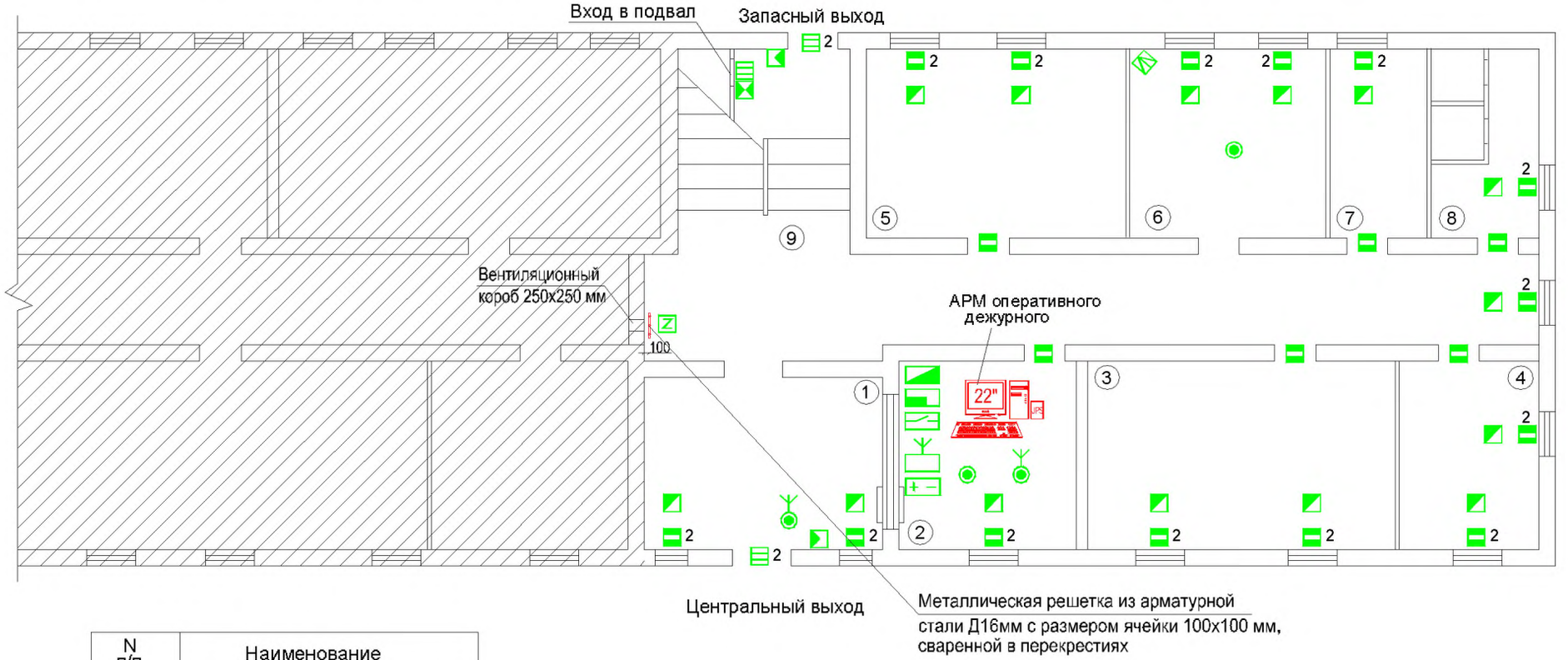


Примечание

Оконечный элемент шлейфа сигнализации установить в конце шлейфа внутри корпуса охранного извещателя или в коробке соединительной КС

Приложение 16

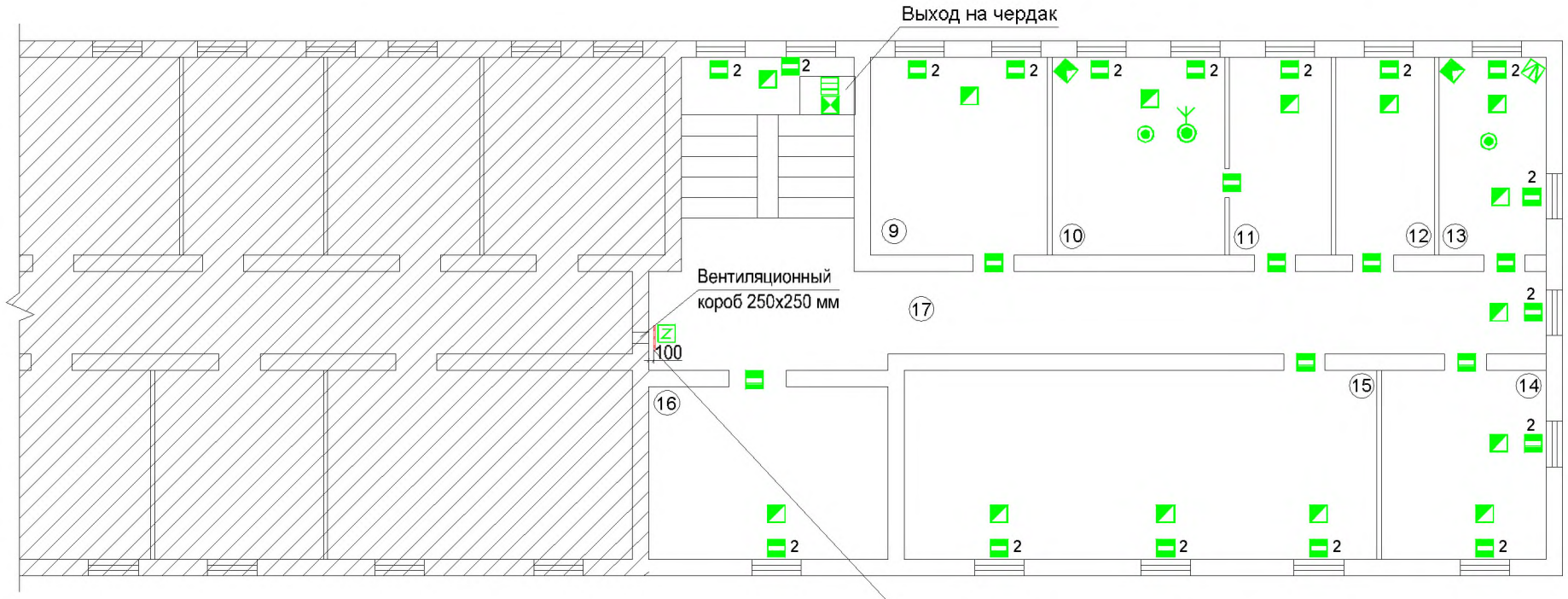
План расположения оборудования СОТС 1-го этажа здания ОВД



N п/п	Наименование
1	Холл
2	Помещение охраны
3	Архив
4	Кабинет
5	Секретариат
6	Спецпомещение
7	Кабинет
8	Сан.узел
9	Коридор

Приложение 17

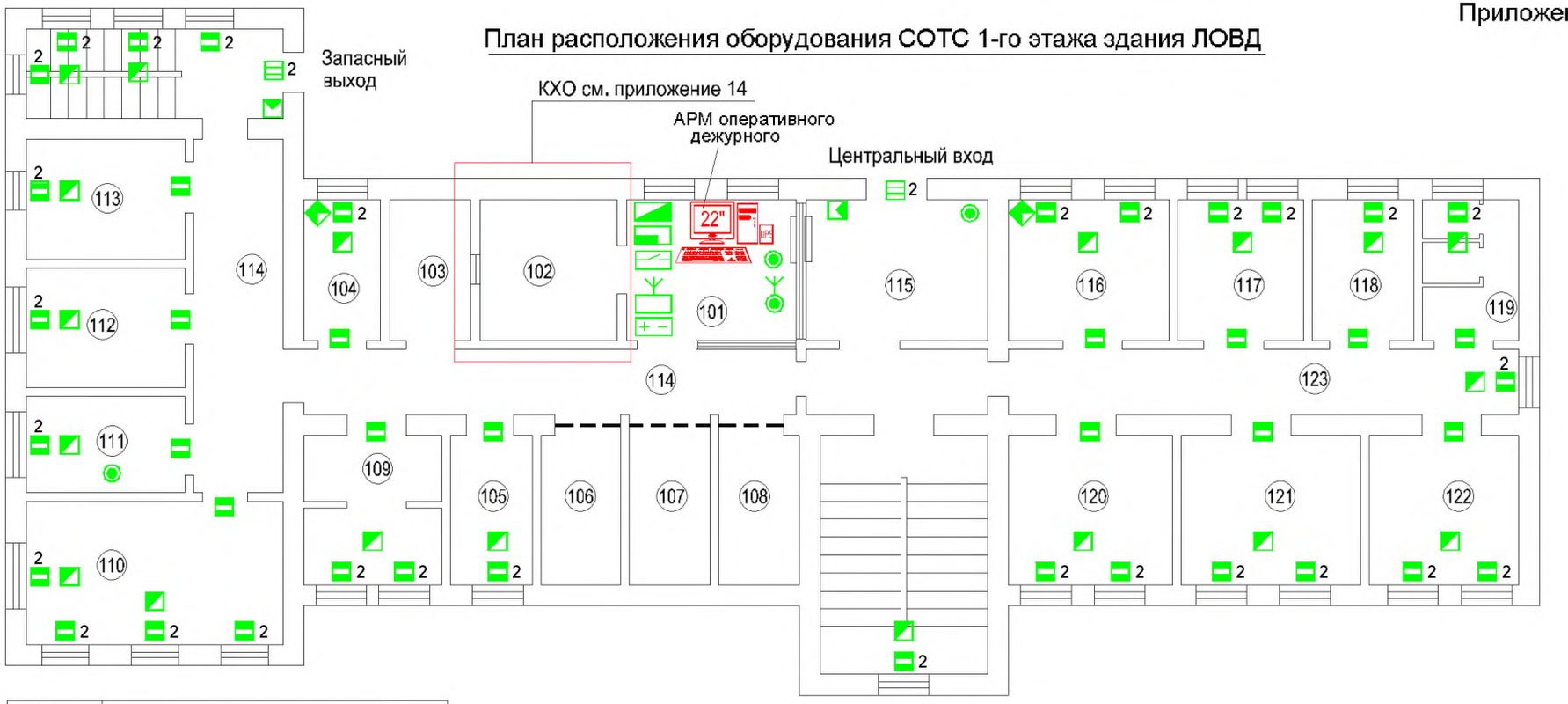
План расположения оборудования СОТС 2-го этажа здания ОВД



N п/п	Наименование
9	Юристконсульт
10	Кабинет начальника
11	Приемная
12	Кабинет
13	Спецпомещение
14	Кабинет
15	Учебный класс
16	Группа кадров
17	Коридор

Приложение 18

План расположения оборудования СОТС 1-го этажа здания ЛОВД



N п/п	Наименование
101	Зал оперативного дежурного
102	Комната хранения оружия
103	Комната чистки оружия
104	Комната для хранения средств защиты, связи, оперативной и криминальной техники
105	Аппаратная
106-108	Специальное помещение для содержания задержанных лиц
109	Сан.узел
110	Комната следственно-оперативной группы
111	Помещение для выявления обстаятельств задержания лиц доставленных в дежурную часть

112	Помещение для размещения конвоя
113	Комната для подогрева и приема пищи
114	Коридор
115	Холл
116	Серверная
117	Кабинет
118	Кабинет
119	Сан.узел
120	Комната старшины
121	Кабинет
122	Кабинет
123	Коридор

Приложение 19

План расположения оборудования СОТС 2-го этажа здания ЛОВД



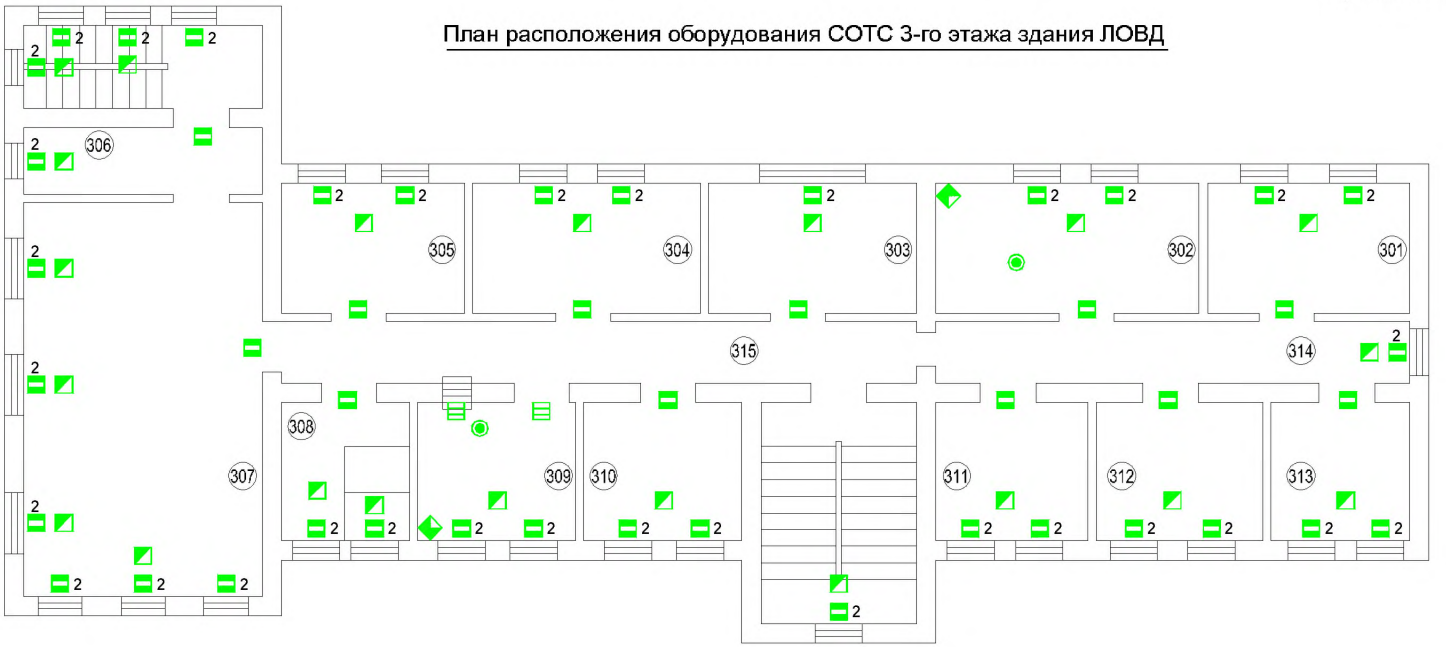
N п/п	Наименование
201	Сан.узел
202	Кабинет
203	Кабинет
204	Кабинет
205	Секретариат
206	Кабинет
207	Коридор
208	Кабинет
209	Коридор
210	Архив

211	ОДиР
212	ОДиР
213	Кабинет оперативного направления
	и мобилизационной готовности
214	Сан.узел
215	Кладовая хранения вещественных
	доказательств
216	Кладовая экспертно-
	криминалистического отдела

217	Кабинет оперуполномоченного
	секретной части
218	Кабинет
219	Кабинет
220	Коридор
221	Коридор

Приложение 20

План расположения оборудования СОТС 3-го этажа здания ЛОВД



N п/п	Наименование
301	Кабинет
302	Секретка (спецпомещение)
303	Холл
304	ФЭО
305	ФЭО
306	Кабинет
307	Актовый зал

308	Сан.узел
309	Касса
310	Кабинет
311,312	Экспертно-криминалистический
	отдел
313	Кабинет
314	Коридор
315	Коридор

Приложение 21

План расположения оборудования СОТС 4-го этажа здания ЛОВД

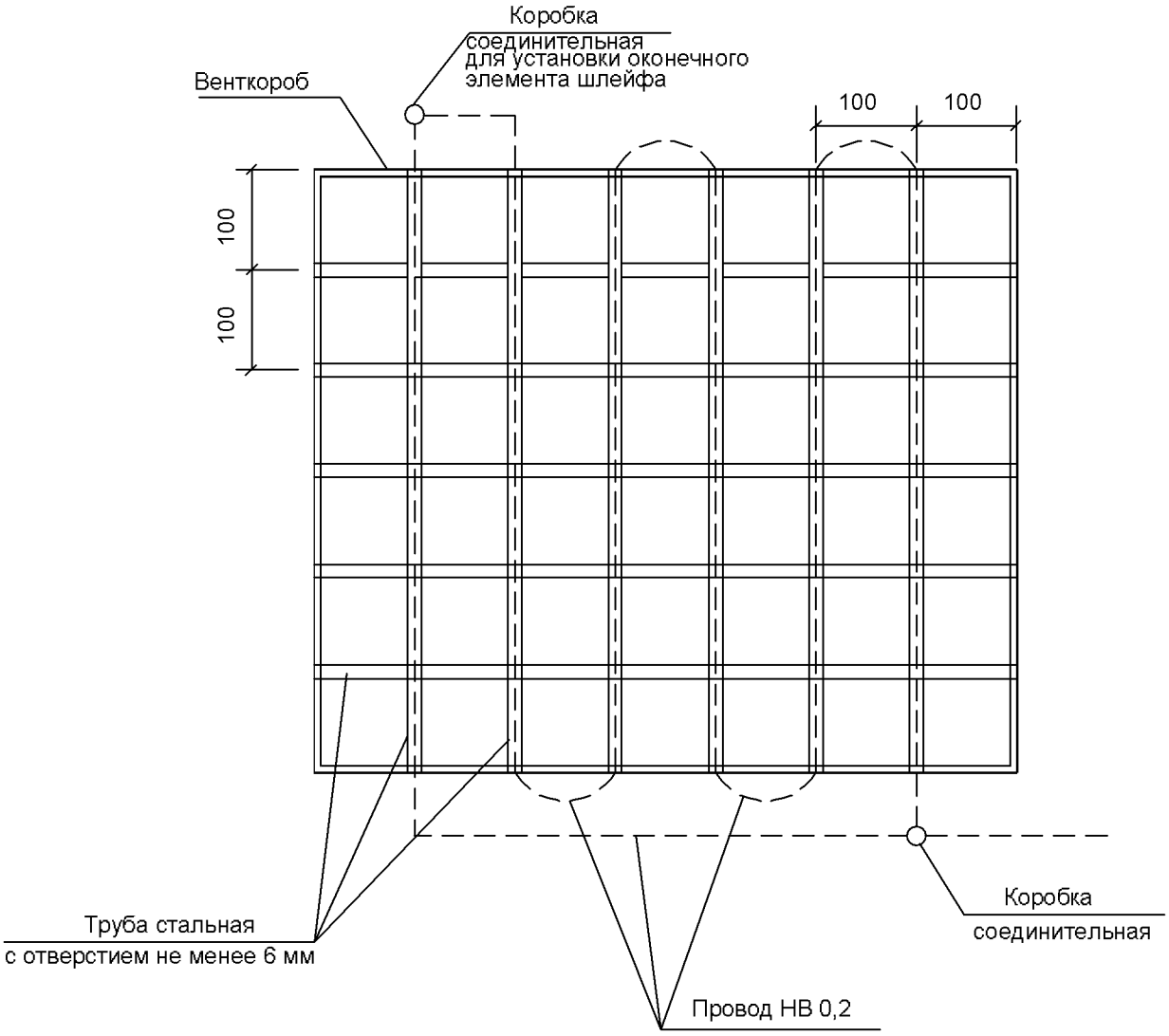


N п/п	Наименование
401	Санузел
402	Кабинет
403	Кабинет
404	Кабинет
405	Кабинет
406	Кабинет
407	Кабинет
408	Кабинет
409	Коридор
410	Отдел кадров
411	Отдел кадров

412	Кабинет
413	Архив
414	Комната отдыха
415	Санузел
416	Кабинет начальника
417	Приемная
418	Кабинет
419	Кабинет
420	Кабинет
421	Коридор
422	Коридор

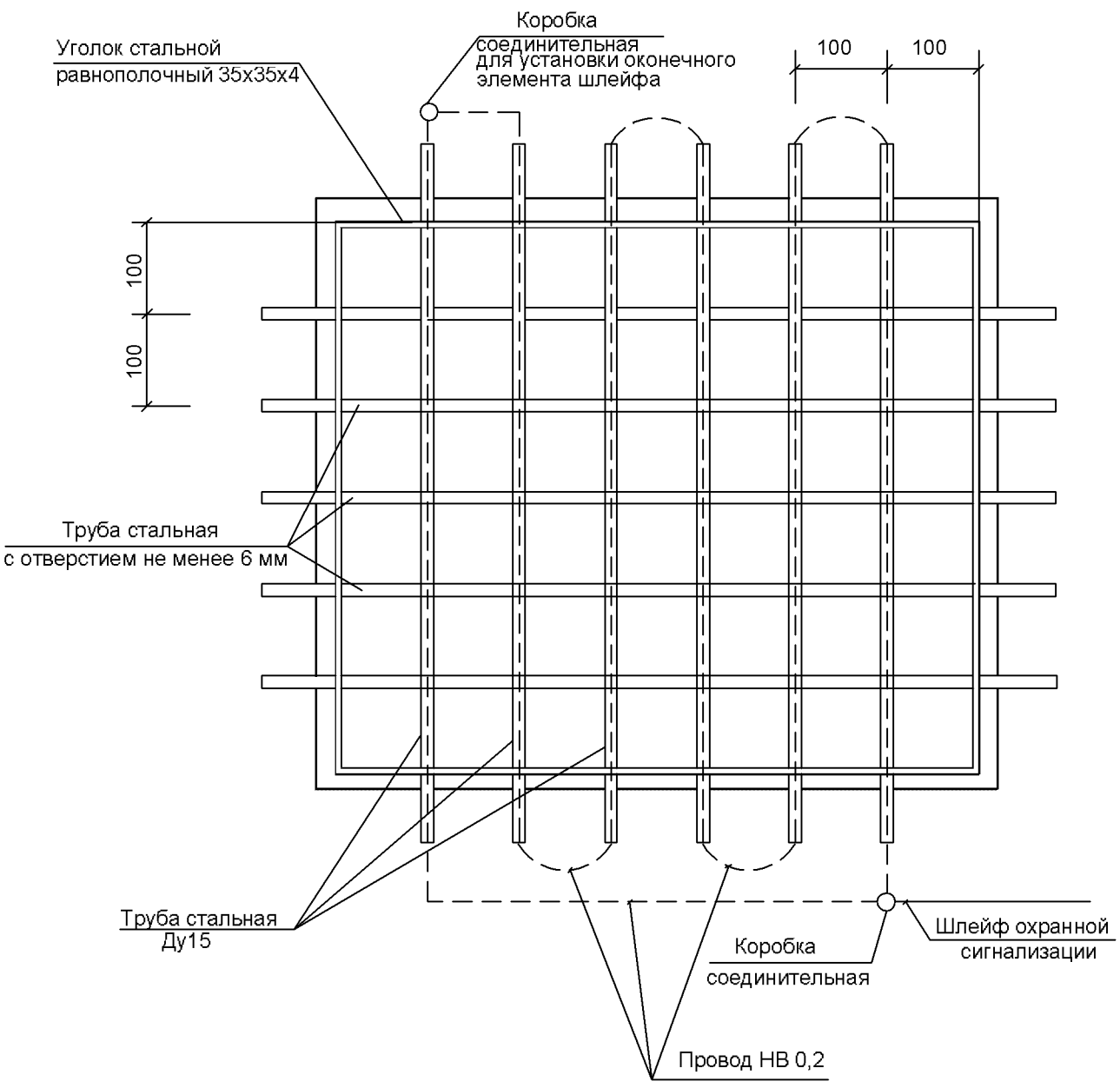
Приложение 22

Схема блокировки венткороба
омическим извещателем



Приложение 23

Схема блокировки окна
омическим извещателем



ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых ко второй категории»

Система охранная телевизионная

РАЗДЕЛ 2

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	60
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	61
3.	СИСТЕМА ОХРАННАЯ ТЕЛЕВИЗИОННАЯ (СОТ)	63
3.1	Типы и виды СОТ. Их назначение и функции	63
3.2	Передача телевизионного сигнала	77
3.3	Расчёт объёма архива видеозаписи	78
3.4	Электропитание СОТ	79
3.5	Заземление	80
3.6	Критерии и принципы выбора СОТ	81
3.7	Общие требования к минимально необходимому составу СОТ	82

ПРИЛОЖЕНИЯ.

Приложение 1.	Условные обозначения.	85
Приложение 2.	План расположения оборудования СОТ 1-го этажа ОВД.	86
Приложение 3.	План расположения оборудования СОТ 2-го этажа ОВД.	87
Приложение 4.	Схема структурная СОТ ОВД.	88
Приложение 5.	План расположения оборудования СОТ 1-го этажа ЛОВД.	89
Приложение 6.	План расположения оборудования СОТ 2-го этажа ЛОВД.	90
Приложение 7.	План расположения оборудования СОТ 3-го этажа ЛОВД.	91
Приложение 8.	План расположения оборудования СОТ 4-го этажа ЛОВД.	92
Приложение 9.	Схема структурная СОТ ЛОВД.	93
Приложение 10.	Схемы установки телевизионных камер на столбах.	94
Приложение 11.	Схемы установки телевизионных камер на стене и потолке.	95

1. ОБЩАЯ ЧАСТЬ

Методические рекомендации по оснащению ведомственных объектов СОТ разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 2.01.2013 № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;

- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 51558-2008 «Системы охранные телевизионные. Общие технические требования и методы испытаний»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- Р 78.36.018–2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- Р 78.36.027-2012 «Рекомендации по применению тепловизионного оборудования в системах охранного телевидения»;
- Р 78.36.029-2014 «Об оснащении ПЦО средствами аудио- и видеонаблюдения»;
- Р 78.36.030-2013 «Применение программных средств анализа видеоизображения в системах охранного телевидения в целях повышения антитеррористической защищённости ПЦО подразделений вневедомственной охраны»;
- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения»;
- Р 78.36.042-2014 «Рекомендации по использованию комплекта оборудования для фиксации и передачи видеоинформации с охраняемого объекта на ПЦО»;
- Р 78.36.049-2015 «Применение оборудования охранных телевизионных систем в условиях ограниченной видимости или других дестабилизирующих факторов»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ - Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

В соответствии с пунктом 4.2 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом II категории по степени потенциальной угрозы понимается обособленное помещение или группа помещений, расположенных в зданиях или сооружениях, не относящихся к системе органов внутренних дел Российской Федерации, в которых внутриобъектовый режим требует осуществления пропускного режима и круглосуточного дежурства.

3. СИСТЕМА ОХРАННАЯ ТЕЛЕВИЗИОННАЯ.

3.1 Типы и виды СОТ. Их назначение и функции.

СОТ – телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений (со звуковым сопровождением или без него), служебной информации и извещений о тревоге с охраняемого объекта.

3.1.1 Типы и виды СОТ.

Аналоговая СОТ – система, в которой видеосигнал от видеокамер до видеомонитора и/или видеорегистратора передаётся в аналоговом виде, не подвергаясь аналого-цифровому преобразованию.

Цифровая СОТ – система, в которой видеосигнал от телевизионных камер (ТК) преобразуется в цифровую форму с помощью аналого-цифрового преобразователя и далее в СОТ обрабатывается в цифровом виде.

Комбинированная СОТ – система, содержащая элементы аналоговой и цифровой СОТ.

Основные общие элементы различных СОТ:

- ТК;
- тепловизор;
- устройства управления и коммутации видеосигналов;
- источник электропитания, в том числе резервного электропитания;
- соединительные линии;
- вспомогательное оборудование.

ТК делятся на:

- аналоговые и цифровые;
- корпусные и бескорпусные;
- для уличного и внутреннего применения;
- стационарные;
- поворотные;
- купольные;

- для применения в особых условиях;
- чёрно-белого и цветного изображения;
- повышенной чувствительности;
- высокого разрешения;
- вандалозащищённые;
- для скрытого наблюдения.

В зависимости от требований, предъявляемых к системе, ТК могут оснащаться различными устройствами: объективами, защитными или декоративными кожухами, термостатами, кронштейнами, поворотными устройствами и т.п.

ТК характеризуется набором параметров:

- формат матрицы;
- разрешающая способность (разрешение в центральной области изображения или объектива);
- чувствительность;
- синхронизация;
- электронный затвор;
- автоматическая регулировка диафрагмы (АРД);
- автоматическая регулировка усиления (АРУ);
- гамма-коррекция видеосигнала (коррекция);



Рисунок 1. ТК различного конструктивного исполнения.

- компенсация «засветки сзади» (компенсация засветки телекамеры при наблюдении за предметом, освещённым сзади ярким светом);
- канал звука;
- напряжение питания;
- автоматический баланс белого;
- стандарт кодирования цветового сигнала.



Рисунок 2. ТК в вандалозащищённом исполнении.



Рисунок 3. Внешний вид охранного извещателя с установленной в нем ТК.



Рисунок 4. Внешний вид пожарного извещателя с установленной в нем ТК.



Рисунок 5. ТК устанавливаемая на подвесном потолке.



Рисунок 6. Установка ТК с ИК-прожектором
на стене здания.



Рисунок 7. Установка ТК на столбе.



Рисунок 8. Поворотные роботизированные ТК.

3.1.2 Тепловизоры.

Применение тепловизионного оборудования в системах СОТ позволяет существенно повысить эффективность таких систем. Тепловизор менее зависим от ряда погодных условий, затрудняющих обнаружение (дождь, туман и т.п.), и позволяет наблюдать перемещение людей и автомобилей в таких условиях, когда обычная СОТ становится неэффективной.

Тепловизор позволяет обнаруживать цели типа «человек» на значительном удалении от рубежа охраны даже при использовании нарушителем маскировочного халата.

Возможности тепловизионного наблюдения в сложных погодных условиях значительно превосходят возможности телевизионного наблюдения.

Совместное применение тепловизоров и ТК является наиболее эффективным средством для обнаружения нарушителей.

Типы тепловизоров:

- стационарные;
- переносные;
- с охлаждением приёмника ИК-излучения;
- без охлаждения приёмника ИК-излучения.



Рисунок 9. Внешний вид стационарного тепловизора.



Рисунок 10. Внешний вид переносного тепловизора.

По типу структуры приёмника тепловизоры разделяются:

- в виде матрицы (например, 328x256 пиксела);
- в виде линейки (например, 288x4 пиксела).

По типу сканирования окружающего пространства:

- с механическим сканированием (при этом обычно применяется приёмник в виде линейки);
- без механического сканирования (при этом обычно применяется приёмник в виде одной или нескольких матриц).

Возможности тепловизора:

- работа в полной темноте;
- регистрация объекта при дожде и снеге.

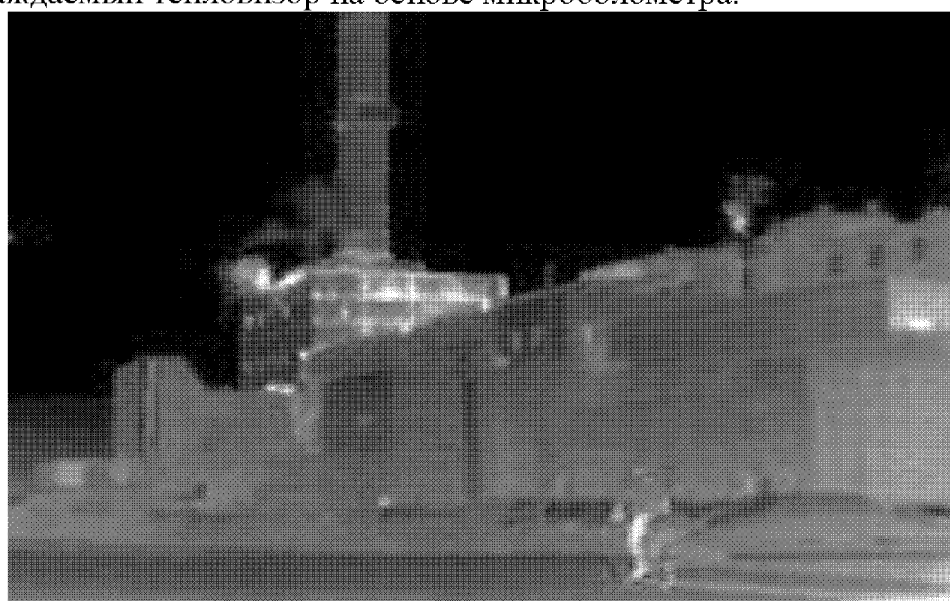
Дальность регистрации объекта при дожде и снеге снижается незначительно, в тумане дальность регистрации объекта падает сильно, поэтому неправильно рассматривать тепловизор как абсолютное средство обнаружения.

Недостатки тепловизора:

Более низкое разрешение изображения, чем у прибора с зарядовой связью[1] (ПЗС-матрица) телевизионной камеры;

- высокая стоимость;
- тенденция к деградации матрицы, особенно для охлаждаемых матриц и сложных соединений типа КРТ[2]. Для болометра[3] на основе оксида ванадия время работы около 40000 часов (4,5 года).

Наиболее приемлемым типом тепловизора для использования является неохлаждаемый тепловизор на основе микроболометра.





[1] ПЗС — прибор с зарядовой связью. Общее обозначение класса полупроводниковых приборов, в которых применяется технология управляемого переноса заряда в объеме полупроводника. Название ПЗС — прибор с зарядовой связью — отражает способ считывания электрического потенциала методом сдвига заряда от элемента к элементу.

[2] КРТ - кадмий-ртуть-теллур.

[3] Болометр - прибор для измерения энергии электромагнитного излучения (главным образом инфракрасного), основанный на изменении электрического сопротивления термочувствительного элемента. в результате поглощения им энергии измеряемого излучения.

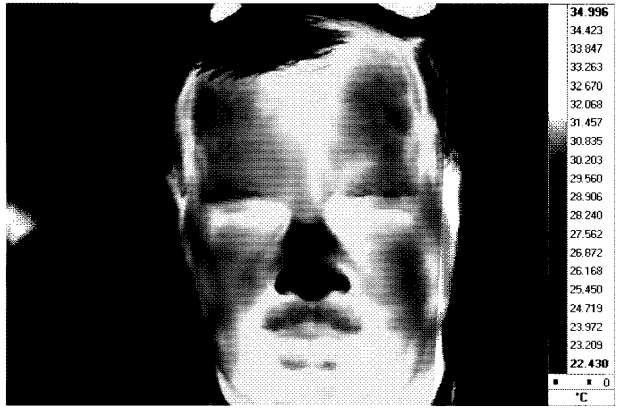


Рисунок 11. Примеры тепловизионных изображений.

3.1.3 Устройства обработки и коммутации видеосигналов.

Устройства обработки и коммутации видеосигналов – это устройства, управляющие потоками информации в СОТ: сигналами изображения, сигналами тревоги и управляющими сигналами. Использование устройств управления и коммутации видеосигналов позволяет существенно облегчить работу оператора, синхронизировать работу СОТ с другими системами безопасности объекта (системами охранно-тревожной сигнализации, контроля и управления доступом и др.).

Устройства обработки и коммутации видеосигналов подразделяются на:

- видеомониторы;
- видеокоммутаторы (Switcher);
- видеоквадраторы (Quadspliter);



Рисунок 12. Пример изображения, полученного тепловизором.



Рисунок 13. Пример изображения, полученного ТК.

- мультиплексоры (Multiplexer);
- матричные коммутаторы (Matrixswitcher);
- видеорегистраторы;
- выполненные на базе персональных и специализированных компьютеров.

3.1.4 Видеомониторы.

К параметрам, характеризующим монитор, относятся:

- диагональ экрана;
- соотношение сторон экрана;
- линейность;
- контрастность;
- яркость;
- строчная частота;
- кадровая частота;
- ширина полосы пропускания видеотракта.

Выбор монитора следует осуществлять таким образом, чтобы его разрешающая способность была выше, чем у применяемых ТК. Монитор не должен ухудшать общее разрешение системы.

3.1.4 Видеоквадраторы и видеокоммутаторы.

Видеоквадратор – это устройство, позволяющее одновременно выводить на экран видеомонитора изображения от четырёх источников видеосигнала, размещая их в соответствующих сегментах экрана.

Видеокоммутатор – это устройство, обеспечивающее последовательное переключение видеосигналов от нескольких ТК на один или несколько выходов (мониторов).

Видеокоммутаторы имеют автоматический и ручной режимы переключения ТК, позволяющие просматривать сигналы от всех ТК либо выборочно от некоторых из них.

Число входных видеоканалов может быть от 4 до 16, а при использовании нескольких блоков коммутации и более.

Видеоквадраторы и видеокоммутаторы для СОТ должны иметь дополнительные тревожные входы для подключения средств сигнализации. Количество дополнительных входов определяется количеством ТК.

Видеоквадраторы и видеокоммутаторы могут быть подключены к системе охранной сигнализации. При поступлении сигнала тревоги на видеоквадраторы и видеокоммутаторы от системы охранной сигнализации они должны выполнять следующие функции:

- вывод изображения в зоне тревоги на полный экран АРМ оператора;
- фиксацию изображения в одном из сегментов;
- передачу звукового сигнала тревоги;
- запись изображения тревожной зоны.

3.1.5 Видеомультиплексоры.

Видеомультиплексоры представляют собой системы видеозаписи и управления, обладающие широкими функциональными возможностями и предназначенные для записи видеосигналов от нескольких ТК на одно записывающие устройство (кодирование), воспроизведение кодированной информации и обработку сигналов тревоги.

Мультиплексоры позволяют осуществлять переключение между различными методами записи, что даёт возможность либо записывать изображение, появляющееся на экране, либо просматривать на экране изображения от одних ТК, записывая в это же время изображения от других ТК. Записанные изображения могут просматриваться на одном мониторе в полноэкранном режиме, режимах квадрированного экрана и "картинка в картинке" либо в мультиэкранном режиме, рисунок 10 (8+2, 9, 4+3, 12+1 или 16 сегментов на одном экране). Для более подробного анализа полноэкранных изображений многие мультиплексоры имеют функцию цифрового увеличения изображения: «ZOOM» (увеличение) позволяет увеличивать участок изображения относительно выбранной точки.



Рисунок 14. Изображение, выведенное на монитор в мультиэкранном режиме.



Рисунок 15. Рабочее место оператора СОТ.

Некоторые видеомультиплексоры имеют:

- возможность вывода изображения от любой подключённой ТК на любой из подключённых (как правило, до 4-х) мониторов;
- «телеметрические» функции (управление внешними устройствами);
- автоматическое и ручное «замораживание» кадра на экране дополнительного видеомонитора;

- контроль пропадания видеосигнала (пропадание входного видеосигнала видеомультиплексор воспринимает как «тревожную» ситуацию);
- цифровое увеличение изображения на экране дополнительного видеомонитора;
- балансировка яркости изображения от всех ТК (создание равно яркого квадрированного изображения);
- встроенные видеодетекторы движения;
- генераторы титров, даты и времени.



Рисунок 16. Образцы квадраторов и мультиплексоров.

3.1.6 Матричные видеокоммутаторы.

Матричный видеокоммутатор – это устройство, обеспечивающее соединение определённого числа ТК с определённым числом абонентов (мониторов, видеорегистраторов).

Главной задачей матричного коммутатора является переключение трансляции изображения (прямого или мультиплексированного) от любой ТК к любому абоненту системы по команде оператора или в автоматическом режиме.

Матричные коммутаторы по виду внутренней обработки видеоинформации делятся на аналоговые и цифровые.

3.1.7 Цифровые СОТ на базе персонального компьютера (ПК).

Типовая СОТ на базе ПК включает в свой состав одну или несколько плат видеозахвата и программное обеспечение (Рисунок 13).



Рисунок 17. Аналоговая система видеонаблюдения.



Рисунок 18. Один из вариантов комплектации СОТ на базе ПК.

3.1.8 СОТ на базе IP-видеонаблюдения.

В IP-видеонаблюдении используются в первом случае персональные компьютеры под управлением стандартной операционной системы (Windows и др.) с установленными специализированными платами «видеозахвата» и программным обеспечением для видеорегистрации, в другом случае цифровые видеорегистраторы являются специализированным оборудованием для IP-видеонаблюдения, устройствами, предназначенными под задачу видеорегистрации, то есть специально разработанное вычислительное устройство с максимально «облегченной» операционной системой (Linux, Windows, Embeded и др.), соответственно, максимально надёжное.

Цифровые гибридные видеорегистраторы позволяют осуществлять:

- видеорегистрацию цветного изображения с разрешением 700Твл;
- скорость регистрации на каждый канал 25 кадров/сек;
- общая скорость регистрации для 16 каналов составляет 400 кадров/сек;

– возможность использования одного из алгоритмов сжатия (M-JPEG, MPEG-2, MPEG-4, H.264).



Рисунок 19. Структурная схема СОТ с применением цифрового гибридного видеорегистратора.

Аналоговая передача сигнала по кабельным линиям подвержена ослаблению, искажению (необратимые потери) и имеет относительно невысокую помехозащищённость.

Для передачи изображения в IP-видеонаблюдении используется протокол TCP/IP и канал передачи информации Ethernet. IP-ТК передаёт видеоизображение в цифровом виде, используя алгоритм сжатия M-JPEG, MPEG-2, MPEG-4, H.264.

Каждое устройство, используемое в системе IP-видеонаблюдения (видеорегистратор, рабочая станция (компьютер) для просмотра видеоизображений), имеет персональный адрес.

В системе IP-видеонаблюдения информация имеет цифровой вид, что позволяет осуществлять её передачу и хранение без потерь.

В данных системах существует возможность использование ТК со сверхвысоким разрешением 1024x720 (720p), 1920x1080 (1080p, Full HD), 3МП (мегапиксела), 4МП, 8МП и т.д.

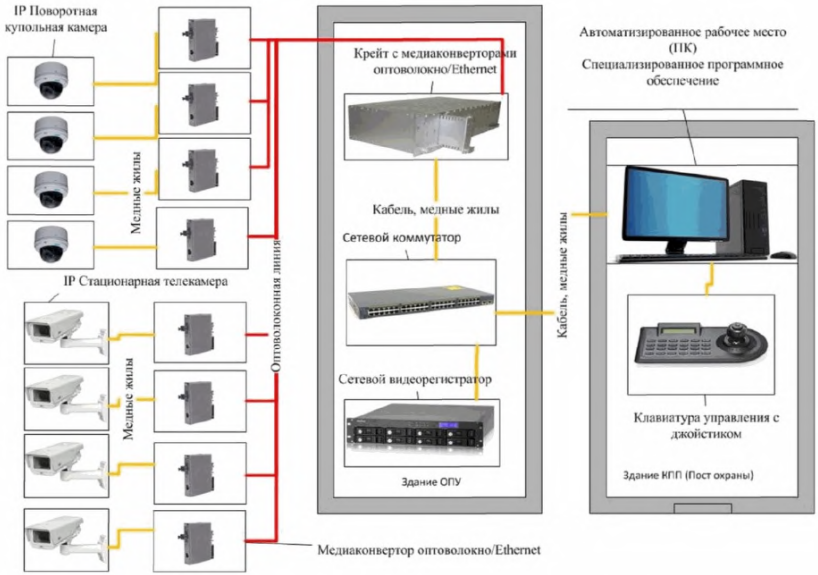


Рисунок 20. Структурная схема СОТ на базе IP-видеонаблюдения.

В системах IP-видеонаблюдения имеются следующие возможности:

- дистанционное конфигурирование параметров IP-ТК;
- тиражирование видеопотоков большому количеству конечных потребителей – «multicasting», что минимизирует трафик в сети и снижает требования к аппаратной части серверов и рабочих станций (компьютеров);
- резервирование магистральных линий связи, что обеспечивает дублирование линий связи между активными коммутационными устройствами (сетевыми коммутаторами, видеорегистраторами и прочими);
- видеонаблюдение и передача видеоинформации (видеопотоков) на большие расстояния через ИСОД (ЕИТКС) МВД России или интернет;
- использование функции Powerover Ethernet (PoE) – электропитание IP-ТК по тому же кабелю («витая пара»), по которому происходит передача видеоданных, что исключает необходимость в прокладке отдельного кабеля питания к каждой телекамере и в случае большой распределенной системы является очень эффективным. (Использование этой возможности предполагает установку сетевого коммутатора с функцией PoE);

– видеорегистрация на iSCSI RAID[4]-массивах, которые подключаются непосредственно к активным коммутационным устройствам – сетевым коммутаторам.

3.1.9 Устройства регистрации.

Реализация цифровых устройств видеорегистрации осуществляется с помощью специализированных видеорегистраторов (DVR) и СОТ на базе ПК.

Преимущества DVR:

– высокая надежность;
– простота в управлении;
– небольшие размеры.

Гибридные DVR – аппараты, способные записывать сигналы одновременно с аналоговых ТК и IP-ТК, при этом не происходит потери качества изображения.

3.2 Передача телевизионного сигнала.

Для передачи телевизионного сигнала в СОТ могут использоваться как проводные каналы связи (коаксиальные кабели, симметричные проводные линии типа «витая пара», телефонные линии, волоконно-оптические линии), так и беспроводные каналы (радиоканал или ИК-канал).

Наиболее стабильная и качественная работа системы обеспечивается при использовании волоконно-оптических линий и коаксиальных кабелей.

Основными характеристиками коаксиального кабеля являются его волновое сопротивление, диаметр (как правило, чем больше диаметр кабеля, тем меньше затухание сигнала в нем) и погонное затухание, эффективность экранирования, степень защиты внешней оболочки (одной из важнейших характеристик является огнестойкость), климатическое исполнение.

Входные и выходные сопротивления основных компонентов СОТ имеют значение 75 Ом, применение кабелей с волновым сопротивлением 75 Ом не допускается.

Использование для передачи видеосигнала оптоволокна полностью исключает наводки на него.

Для передачи сигнала по кабелю «Витая пара» необходимо использование специального оборудования (приёмник и передатчик сигнала).

Преимущества передачи сигнала по «витой паре»:

– помехозащищённость линий передачи от низкочастотных помех (в первую очередь от сетевой наводки в 50 Гц);
– увеличение длины линии трансляции: для цветного видеосигнала составляет до 1000 м, для черно-белого – до 2000 м.

---

[4]RAID — массив из нескольких дисков, управляемых контроллером, связанных между собой скоростными каналами передачи данных и воспринимаемых внешней системой как единое целое. В зависимости от типа используемого массива может обеспечивать различные степени отказоустойчивости и быстродействия.

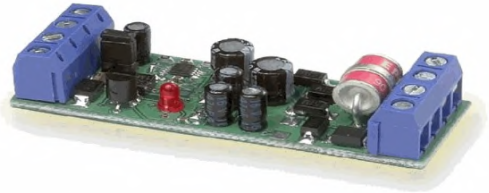


Рисунок 21. Передатчик видеосигнала по витой паре.



Рисунок 22. Приемник видеосигнала по витой паре.

Недостатки кабеля типа «витая пара»:

- искажение исходного видеосигнала по сравнению с коаксиальным кабелем;
- использование видеоусилителей и модемов (передатчики-модуляторы и приёмники-демодуляторы) для передачи сигнала на большие расстояния;
- использование на линиях передачи видеосигнала устройств грозозащиты.

3.3 Расчёт объёма архива видеозаписи.

На размер объёма архива видеозаписи существенно влияет ряд факторов:

- индивидуальная настройка для каждой ТК;
- осуществление цифровой мультиплексной записи одновременно по всем ТК;
- программирование приоритета при записи тревожных событий;

- программирование времени и скорости записи предтревожной ситуации;
- программирование режимов записи в зависимости от приходящих внешних сигналов тревоги и наличия движения в кадре.

Запись событий может включаться по сигналу тревоги на заданное время, сохранять одиночный кадр или вестись непрерывно.

Расчёт архива хранения сводится к определению размера кадра изображения, темпа записи кадров в секунду на каждую ТК, необходимого интервала времени для записи. Все эти данные определяются по согласованию с Заказчиком.

Пример расчёта объема архива записи при записи в режиме реального времени.

Разрешение ТК	Темп записи, кадр/сек	Размер кадра, кБ	Объём архива на камеру за день, ГБ	Количество записываемых ТК	Архив, дней	Общий объём архива, ТБ
704x576	25	13	28,08	16	30	13,48

Применяемые жёсткие диски в устройствах архивирования видеозаписей должны обеспечивать непрерывную работу не менее, чем 3 года, при условии круглосуточной видеозаписи информации от всех ТК.

3.4 Электропитание СОТ.

Электропитание СОТ осуществляется по 1 категории от отдельной группы щита дежурного освещения переменным током напряжением 220 В, 50 Гц.

При пропадании основного электропитания СОТ должна автоматически переходить на электропитание от резервного источника электропитания.

Согласно требованию п. 5.9.8. ГОСТ Р 51558-2014 при переходе на электропитание от резервного источника электропитания должна обеспечиваться бесперебойная работа системы не менее 0,5 часа.

Пример расчёта бесперебойного источника питания напряжением 220 В, 50 Гц.

	Наименование	Кол-во, шт.	Потребляемая мощность, ВА	Суммарная потребляемая мощность,

				ВА
1	Монитор 22”	1	250	250
2	Цифровой видеорегистратор	1	250	250
3	Коммутатор	1	40	40
4	Источник питания для ТК	1	200	200
5	ИТОГО			740

Q(Ач) = Pp/U x t(ч)x1,2,

где:

Pp - потребляемая мощность СОТ 740 ВА;

U- выходное напряжение аккумуляторов 12 В;

t - требуемое время работы 0,5 ч;

1,2 - коэффициент запаса ёмкости.

Необходимая ёмкость источника электропитания напряжением 220 В составляет:

740 ВА/12 В x 1,2 x 0,5 ч = 37 Ач.

Согласно расчётам, выбирается бесперебойный источник электропитания напряжением 220 В, 50 Гц, удовлетворяющий следующим характеристикам:

– минимальная нагрузка источника не менее 740 ВА;

– ёмкость аккумуляторных батарей должна быть не менее 37 Ач.

Электропитание всех элементов СОТ необходимо осуществлять от одной и той же фазы силовой сети.

3.5 Заземление.

Технические решения, использованные при заземлении, во многом определяют качество работы СОТ. При организации заземления необходимо руководствоваться следующими принципами:

Аппаратура СОТ должна быть заземлена, зануление аппаратуры СОТ недопустимо.

Приборы гальванической развязки включаются в разрыв кабельной линии связи, разрывая паразитный контур заземления.

Заземление оборудования и устройств должно выполняться в соответствии с требованиями СНиП 3.05.06-85, ПУЭ, технической документации предприятий-изготовителей.

3.6 Критерии и принципы выбора СОТ.

Выбор системы следует производить с учётом необходимой информативности СОТ, характеристик охраняемого объекта (расположение

на местности, освещённость и другие признаки) и возможных объектов наблюдения (человек, автомобиль и другие цели).

Следует предусмотреть использование ТК, монтируемых в герметичных термокожухах, имеющих солнцезащитный козырёк и ориентированных на местности под углом к линии горизонта во избежание попадания лучей восходящего и заходящего солнца в объектив ТК.

Высота установки и тип крепления ТК должны исключать возможность их умышленного повреждения.

Для организации наблюдения территории в тёмное время суток необходимо предусмотреть систему охранного электроосвещения с учётом системы электроосвещения объекта и применения ТК с инфракрасной подсветкой.

Для наблюдения ТК протяжённых участков территорий объекта в проекте следует предусмотреть совместно с ТК объективы с переменным фокусным расстоянием и/или поворотные устройства и трансфокаторы с дистанционным управлением.

Уличные ТК должны комплектоваться объективами с автоматической регулировкой диафрагмы.

Для отображения поступающей с ТК информации необходимо предусмотреть применение специальных мониторов, работающих круглосуточно в течение длительного времени с неподвижным изображением.

ТК должны быть установлены так, чтобы исключить образование мёртвых зон, не контролируемых ТК.

Для записи телевизионных изображений следует предусмотреть применение цифровых видеорегистраторов.

Система охранная телевизионная с цифровым видеонакопителем должна аппаратно обеспечивать получение кадра на выходе системы не менее 720 х 576 пикселей.

Конструктивно СОТ должна строиться по модульному принципу и обеспечивать:

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

Для повышения вероятности обнаружения попыток проникновения следует использовать программные модули видеоаналитики.

3.7 Общие требования к минимально необходимому составу СОТ.

3.7.1 Минимально необходимый состав СОТ.

Объекты органов внутренних дел Российской Федерации, отнесённые к второй категории, должны быть оборудованы СОТ.

Видеонаблюдение должно осуществляться:

– за периметром зданий и сооружений объекта, их входов и выходов;
– за специальными помещениями и подходами к ним).

ТК устанавливаются на контрольно-пропускном пункте:

– для видеонаблюдения за входной дверью со стороны внешней территории;
– для видеонаблюдения за входной дверью со стороны внутренней территории;
– для видеонаблюдения внутри пропускного коридора;
– для видеонаблюдения за действиями сотрудника, несущего службу на контрольно-пропускном пункте.

В помещении дежурного по контрольно-пропускному пункту и в дежурной части устанавливаются мониторы.

3.7.2 Функции СОТ.

СОТ должна выполнять следующие функции:

– оперативный доступ к видеозаписи и видеоархиву путём установления времени, даты и идентификатора телевизионной камеры;
– разграничение полномочий доступа к управлению системой в целях предотвращения несанкционированных действий;
– активирование телевизионных камер по сигналам охранной сигнализации или видеодетекторов движения;
– обнаружение оставленных (принесённых) предметов;
– определение направления движения объекта в зоне контроля;
– идентификация личности по образу лица;
– распознавание и регистрацию автотранспорта и автомобильных номеров;
– отображение видеоинформации в режиме реального времени;
– запись видеоинформации в режиме 25 кадров в секунду по каждому каналу (с каждой ТК) при максимальном качестве видеоданных;
– просмотр видеоархива любой телевизионной камеры без остановки записи;
– хранение видеоинформации в течение не менее 30 суток;
– приём видеоинформации, передаваемой по сети «Ethernet», одновременно с сообщениями, командами управления и речевыми переговорами;
– включение в локальную сеть нескольких автоматизированных рабочих мест;
– видеонаблюдение;
– видеонаблюдение в ночное время;

- подключение уличных купольных (управляемых) полноприводных цветных ТК с переключением режимов день/ночь;
- вывод видеоинформации от любой ТК на любое автоматизированное рабочее место по команде оператора или по событию в системе охранно-тревожной сигнализации и системе контроля и управления доступом (тревожной ситуации).

Примечания:

1. Аттестованные помещения, а также помещения, предназначенные для обработки сведений, составляющих государственную тайну, оборудуются техническими средствами, прошедшими сертификацию по стандартам ФСТЭК России и ФСБ России.

2. В случае отсутствия (с учетом объективных факторов) на объекте необходимых средств инженерно-технической укреплённости (решётки на окнах и т.д.) либо оснащённости объекта средствами инженерно-технической укреплённости более низкого класса защиты, рекомендуется оборудовать объект дополнительными рубежами охраны с использованием средств охранной сигнализации и СОТ.

Организация дополнительных рубежей охраны должна быть согласована с подразделением охраны и руководством объекта.

ПРИЛОЖЕНИЯ

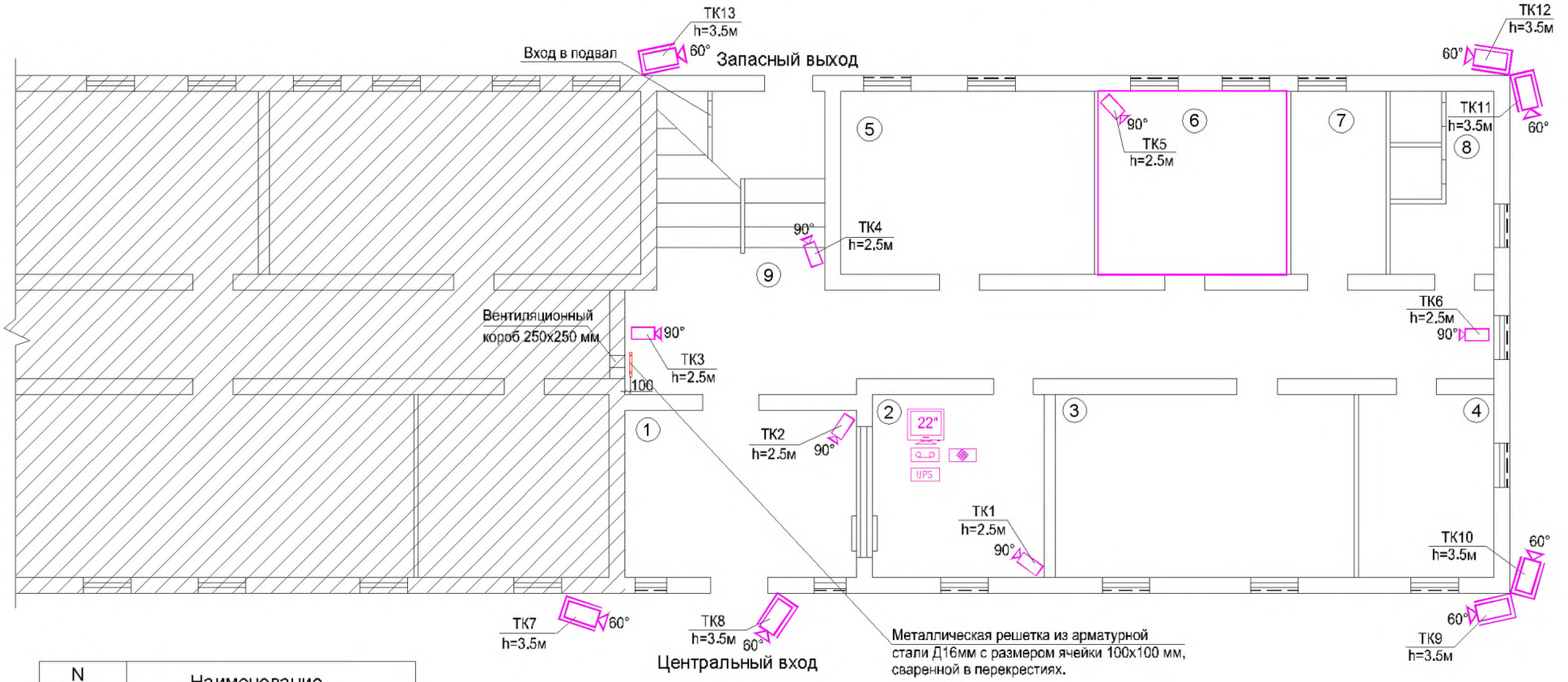
Приложение 1

Условные обозначения

Наименование	Обозначение	
	на планах	на схемах
Видеомонитор		
Видеокамера, установленная в термокожухе, с обозначением угла обзора		
Видеокамера с обозначением угла обзора Видеокамера с обозначением угла обзора		
Коммутатор		
Видеорегистратор		
Источник питания 12В для видеокамер		
Источник бесперебойного питания, 220В,50Гц		

Приложение 2

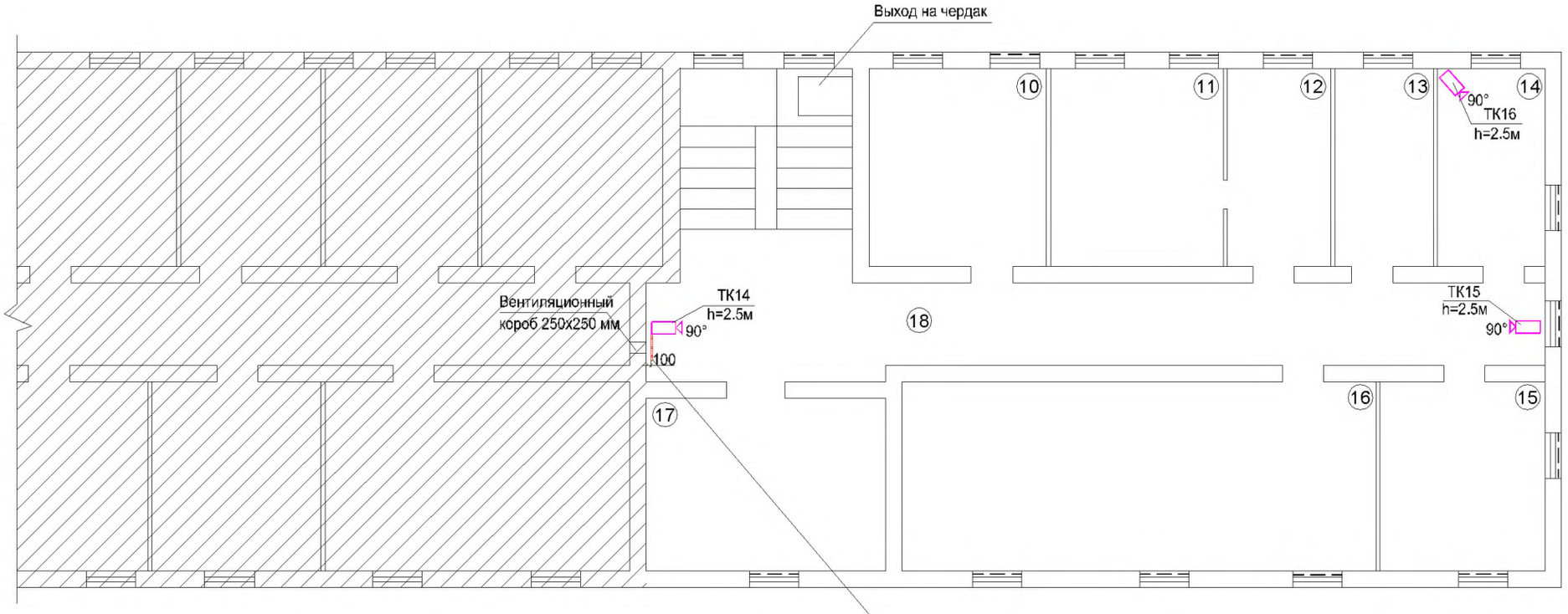
План расположения оборудования СОТ 1-го этажа ОВД



N п/п	Наименование
1	Холл
2	Помещение охраны
3	Архив
4	Кабинет
5	Секретариат
6	Спецпомещение
7	Кабинет
8	Сан.узел
9	Коридор

Приложение 3

План расположения оборудования СОТ 2-го этажа ОВД

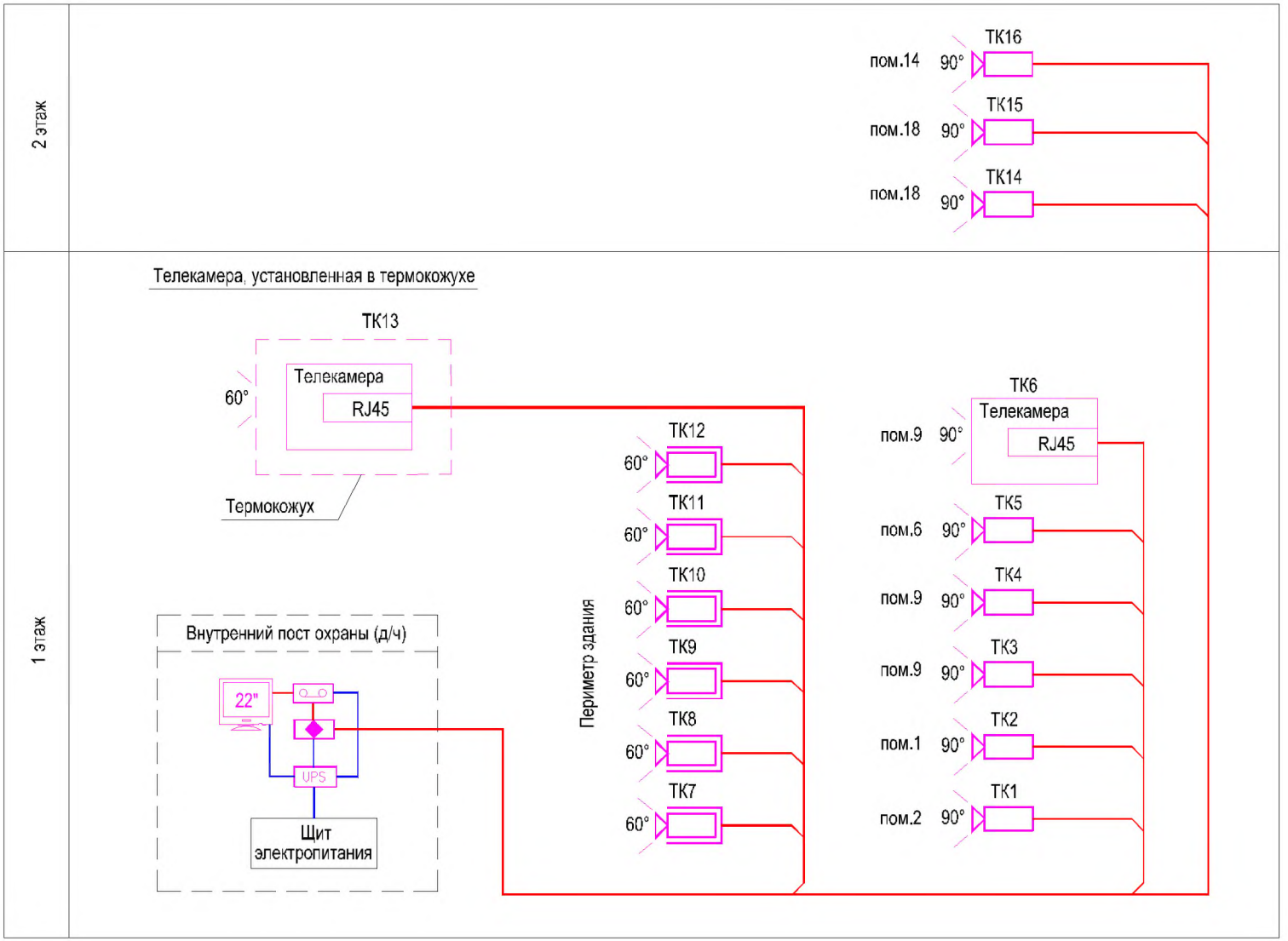


N п/п	Наименование
10	Юристконсульт
11	Кабинет начальника
12	Приемная
13	Кабинет
14	Спецпомещение
15	Кабинет
16	Учебный класс
17	Группа кадров
18	Коридор

Приложение 4

Структурная схема СОТ ОВД

СОТ построена с использованием сетеых телевизионных камер с передачей электропитания PoE.



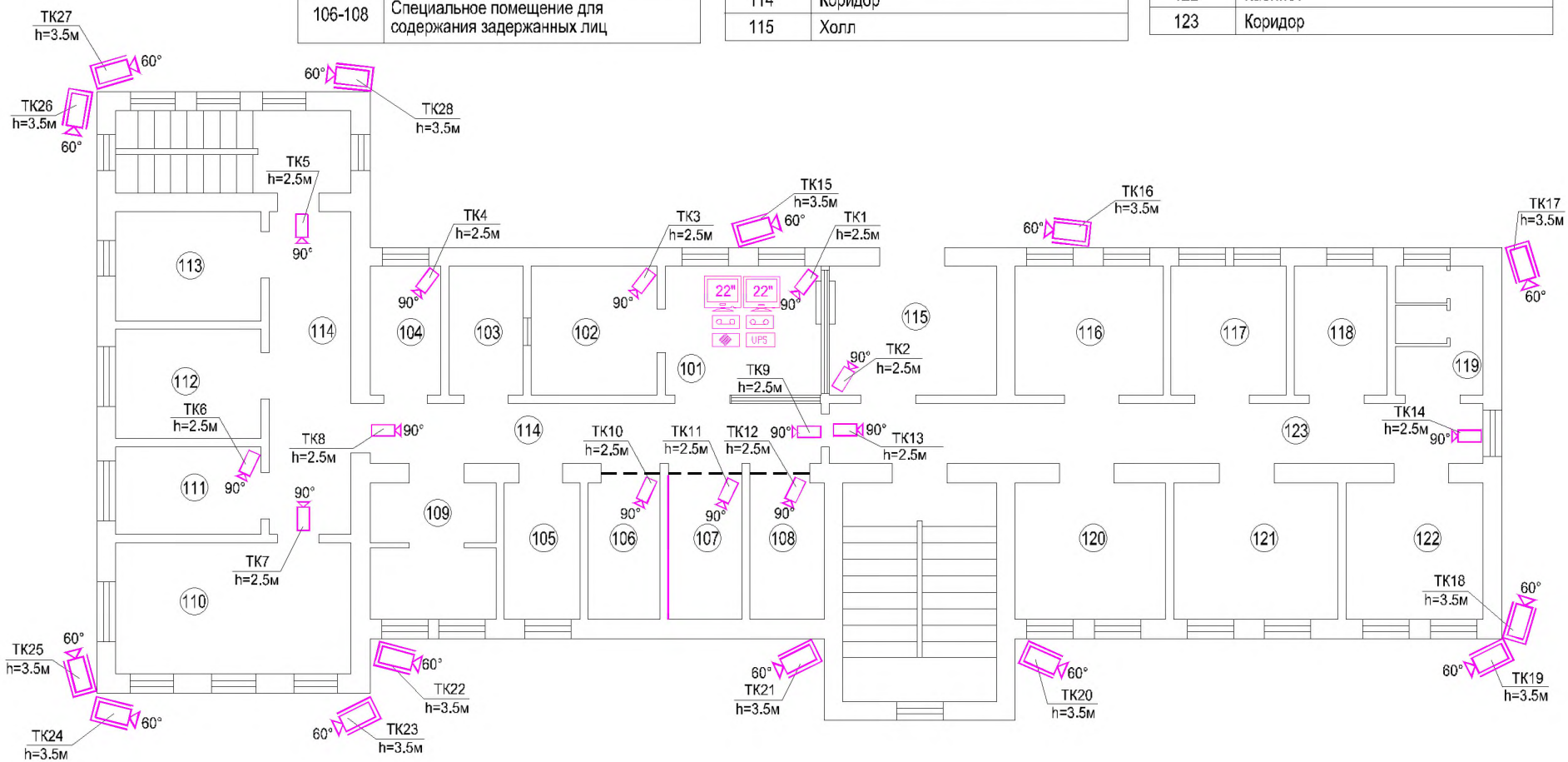
Приложение 5

План расположения оборудования СОТ 1-го этажа ЛОВД

N п/п	Наименование
101	Зал оперативного дежурного
102	Комната хранения оружия
103	Комната чистки оружия
104	Комната для хранения средств защиты, связи, оперативной и криминальной техники
105	Аппаратная
106-108	Специальное помещение для содержания задержанных лиц

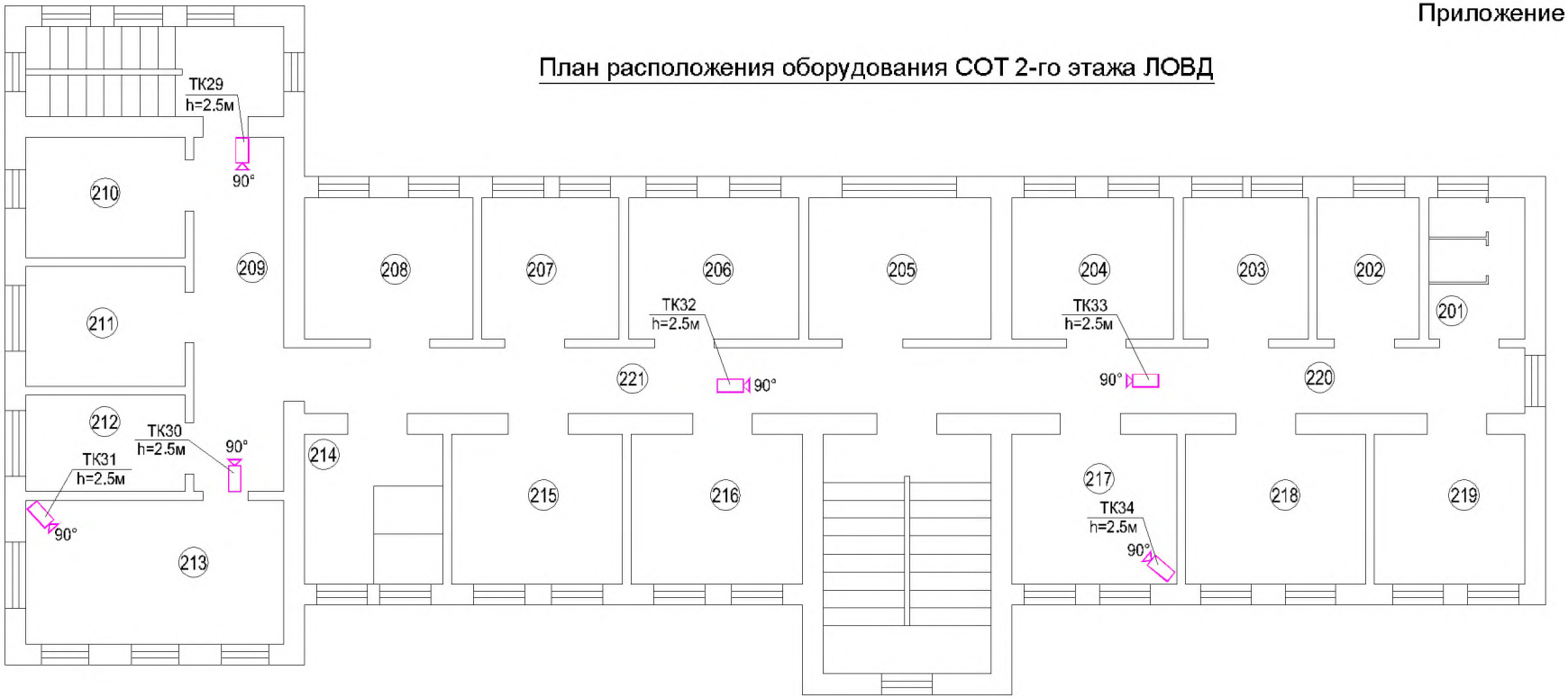
109	Сан.узел
110	Комната следственно-оперативной группы
111	Помещение для выявления обстаятельств задержания или доставление лиц, доставленных в дежурную часть
112	Помещение для размещения конвоя
113	Комната для подогрева и приема пищи
114	Коридор
115	Холл

116	Серверная
117	Кабинет
118	Кабинет
119	Сан.узел
120	Комната старшины
121	Кабинет
122	Кабинет
123	Коридор



Приложение 6

План расположения оборудования СОТ 2-го этажа ЛОВД



N п/п	Наименование
201	Сан.узел
202	Кабинет
203	Кабинет
204	Кабинет
205	Секретариат
206	Кабинет
207	Коридор
208	Кабинет
209	Коридор
210	Архив
211	ОДиР
212	ОДиР

213	Кабинет оперативного направления
	и мобилизационной готовности
214	Сан.узел
215	Кладовая хранения вещественных
	доказательств
216	Кладовая экспертно-
	криминалистического отдела
217	Кабинет оперуполномоченного
	секретной части
218	Кабинет
219	Кабинет
220	Коридор
221	Коридор

Приложение 7

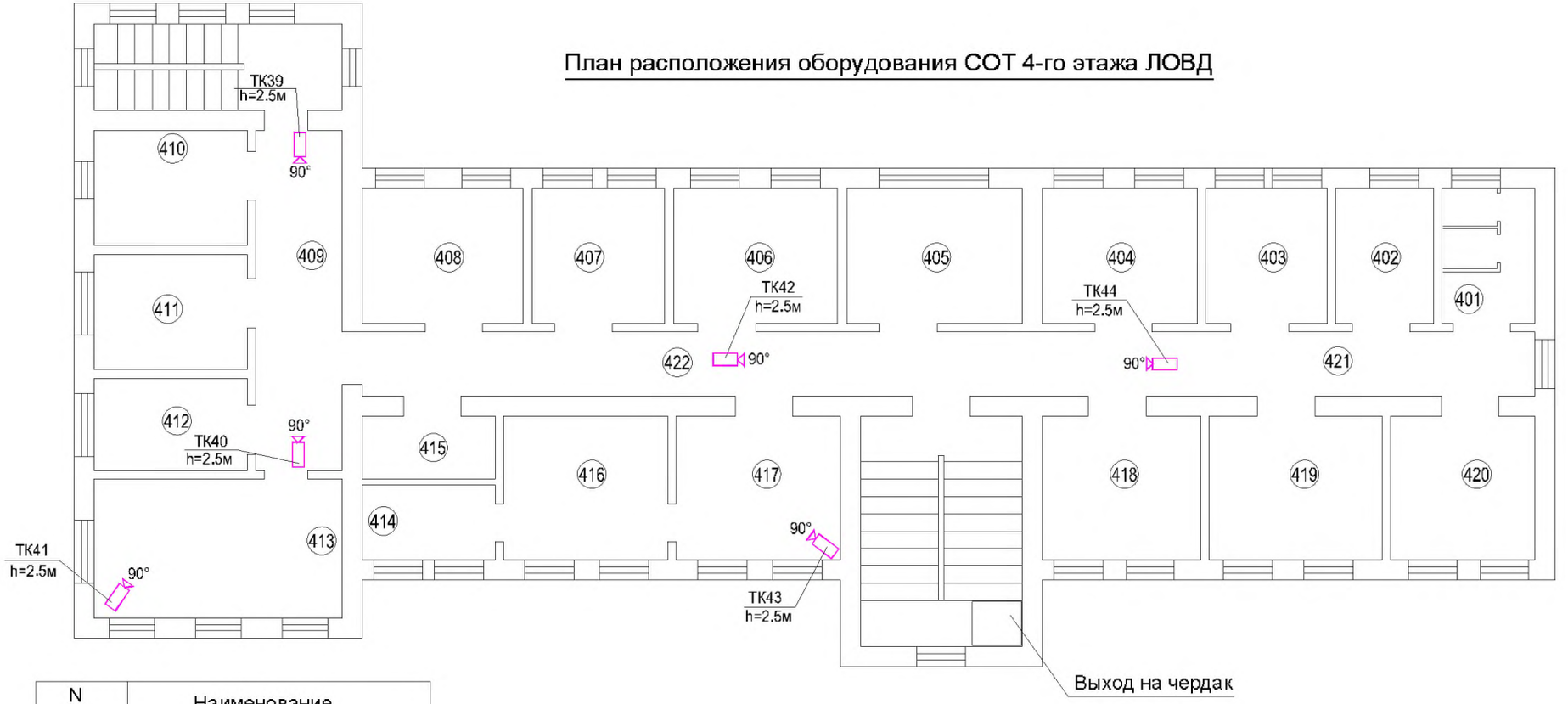
План расположения оборудования СОТ 3-го этажа ЛОВД



N п/п	Наименование
301	Кабинет
302	Секретка (спецпомещение)
303	Холл
304	ФЭО
305	ФЭО
306	Кабинет
307	Актовый зал

308	Сан.узел
309	Касса
310	Кабинет
311,312	Экспертно-криминалистический
	отдел
313	Кабинет
314	Коридор
315	Коридор

План расположения оборудования СОТ 4-го этажа ЛОВД



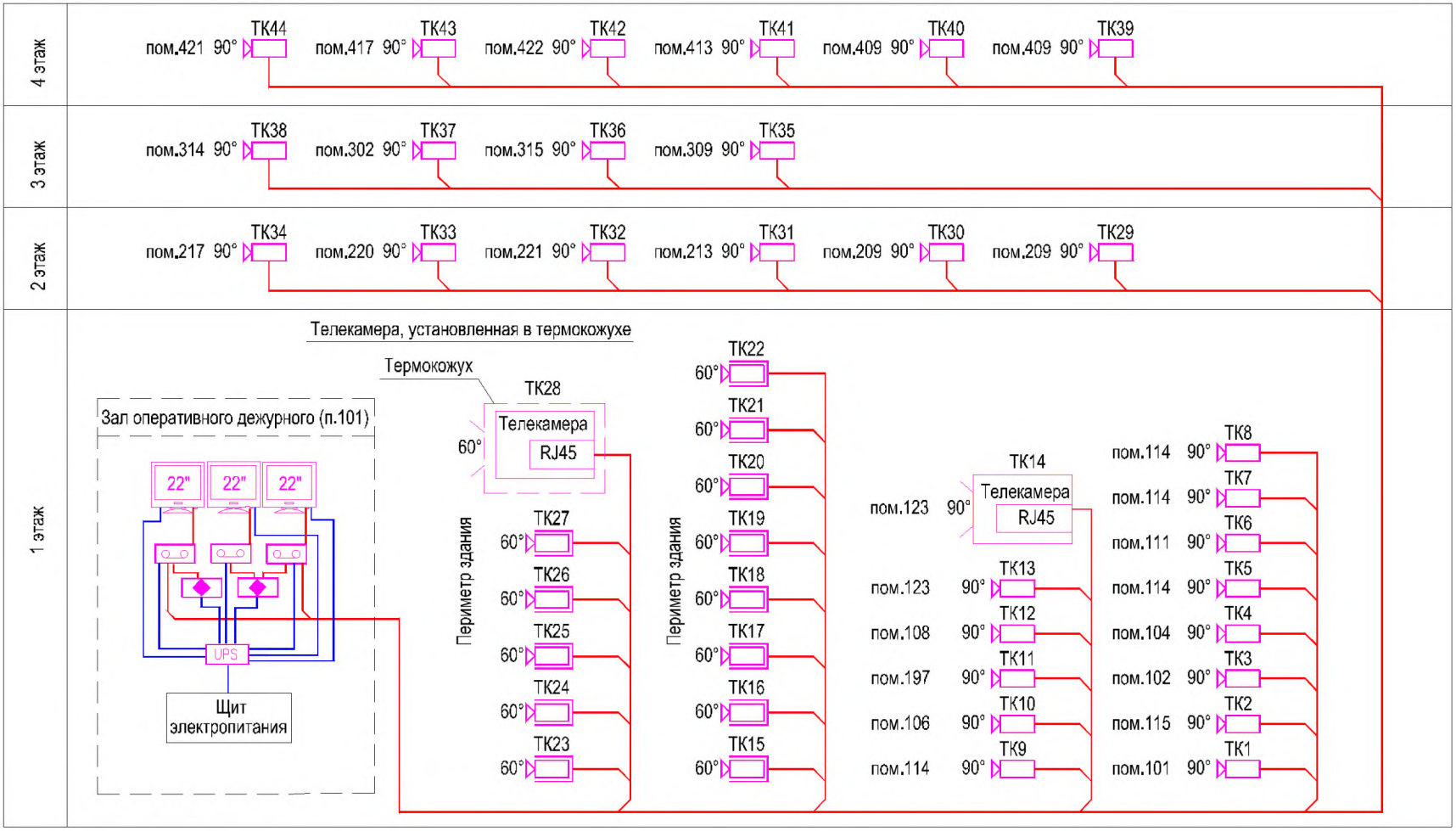
N п/п	Наименование
401	Сан.узел
402	Кабинет
403	Кабинет
404	Кабинет
405	Кабинет
406	Кабинет
407	Кабинет
408	Кабинет
409	Коридор
410	Отдел кадров
411	Отдел кадров

412	Кабинет
413	Архив отдела кадров
414	Комната отдыха
415	Туалет
416	Кабинет начальника
417	Приемная
418	Кабинет
419	Кабинет
420	Кабинет
421	Коридор
422	Коридор

Приложение 9

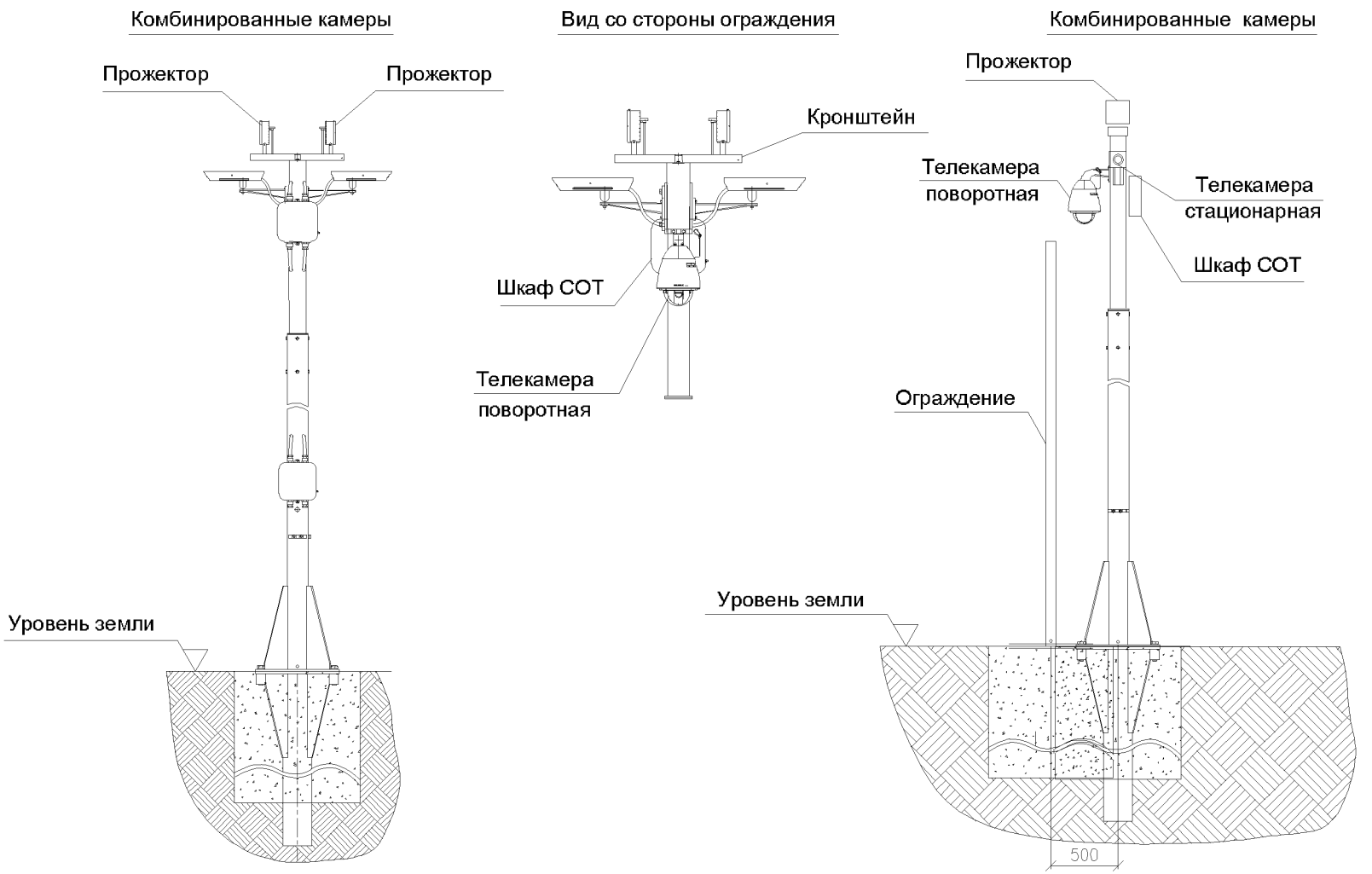
Структурная схема СОТ ЛОВД

СОТ построена с использованием сетеых телевизионных камер с передачей электропитания PoE.



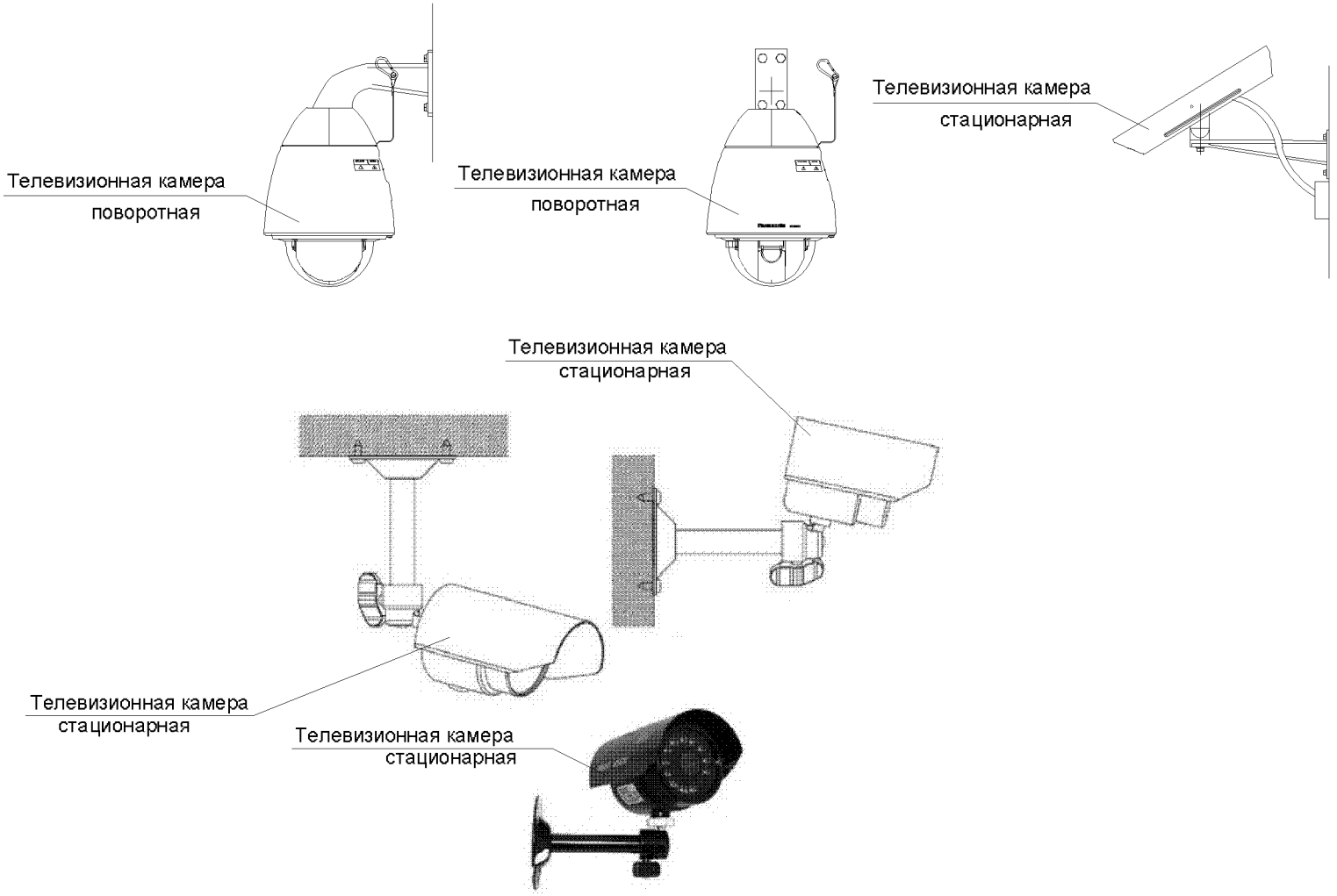
Приложение 10

Схемы установки телевизионных камер на столбах



Приложение 11

Схемы установки телевизионных камер на стене и потолке



ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых ко второй категории»

Система контроля и управления доступом

РАЗДЕЛ 3

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	98
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	99
3.	СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ (СКУД)	100
3.1.	Типы и виды СКУД их назначение и функции	100
3.2.	Функции СКУД в составе систем противокриминальной защиты объектов	102
3.3	Классификация СКУД	102
3.4	Составляющие СКУД	104
3.5	Электропитание СКУД	116
3.6	Выбор СКУД для оборудования объекта	117
3.7	Размещение и монтаж СКУД	118
3.8	Требования к минимально необходимому составу СКУД	121

ПРИЛОЖЕНИЯ

Приложение 1.	Условные обозначения.	125
Приложение 2.	План расположения оборудования СКУД 1-го этажа ОВД.	126
Приложение 3.	План расположения оборудования СКУД 2-го этажа ОВД.	127
Приложение 4.	План расположения оборудования СКУД 1-го этажа ЛОВД.	128
Приложение 5.	План расположения оборудования СКУД 2-го этажа ЛОВД	129
Приложение 6.	План расположения оборудования СКУД 3-го этажа ЛОВД	130
Приложение 7.	План расположения оборудования СКУД 4-го этажа ЛОВД	131
Приложение 8.	Схема установки средств СКУД на одностворчатой двери.	132
Приложение 9.	Схема установки средств СКУД на двустворчатой двери.	133

1. ОБЩАЯ ЧАСТЬ.

Методические рекомендации по оснащению ведомственных объектов СКУД разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 25 июля 2011 г. № 876 «Специальные технические требования по инженерно-технической укреплённости изоляторов временного содержания подозреваемых и обвиняемых органов внутренних дел»;
- приказ МВД России от 2.01.2013 N 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);

- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;
- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- Р 78.36.005-2011 «Выбор и применение систем контроля и управления доступом»;
- Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- РД 78.145-93 «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приёмки работ»;
- Пособие к РД 78.145-93;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану: Методические рекомендации»;
- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Рекомендован решением расширенного заседания Технического совета ГУВО МВД России Протокол № 2 от 9.10.2015);
- ПУЭ - Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА.

В соответствии с пунктом 4.2 Инструкции по обеспечению инженерно-технической укрепленности и повышению уровня антитеррористической защищенности объектов органов внутренних дел Российской Федерации

от преступных посягательств, утвержденной приказом от 31.12.2014 г. № 1152 под объектом II категории по степени потенциальной угрозы понимается обособленное помещение или группа помещений, расположенных в зданиях или сооружениях, не относящихся к системе органов внутренних дел Российской Федерации, в которых внутриобъектовый режим требует осуществления пропускного режима и круглосуточного дежурства.

Например:

Вариант 1 (примерные схемы размещения СКУД приведены в приложениях № 2-3).

Объект: обособленная группа помещений с отдельным входом, занимаемая подразделением МВД России (далее – помещения), расположена в трехэтажном здании в правой его части на первом и втором этажах. Помещения отделены капитальными перегородками.

Здание не относится к системе органов внутренних дел Российской Федерации.

Ограждение прилегающей территории к зданию отсутствует.

Проход по лестнице со второго на третий этаж здания заблокирован металлической дверной конструкцией.

На входе в здание оборудован контрольно-пропускной пункт (КПП) для обеспечения установленного режима доступа людей.

Помещения, отнесенные ко II категории, оборудованы следующими ТСО:

- системой охранно-тревожной сигнализации (СОТС);
- системой охранной телевизионной (СОТ);
- системой контроля и управления доступом.

Вариант 2 (примерные схемы размещения СКУД приведены в приложениях № 4-7).

Объект: обособленные помещения, расположены в четырехэтажной пристройке к зданию, с первого по четвертый этажи, чердачные и подвальные помещения отсутствуют. Здание не относится к системе МВД России, ограждение прилегающей территории не установлено.

На первом этаже здания располагается комната хранения оружия.

Инженерно-техническая укрепленность помещений полиции соответствует II категории.

На центральном входе в здание оборудован КПП.

Помещения оснащены СОТС, СОТ, СКУД.

3. СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ.

Система контроля и управления доступом – совокупность программно-технических средств и организационно-методических мероприятий для санкционированного доступа в помещения (зоны) охраняемого объекта и регистрации фактов доступа и попыток несанкционированного доступа,

а также оперативный контроль за санкционированным доступом на территории охраняемого объекта.

3.1 Типы и виды СКУД. Их назначение и функции.

СКУД классифицируются по:

- способу управления;
- по количеству контролируемых точек доступа;
- по функциональным характеристикам;
- по уровню защищённости системы от несанкционированного доступа к информации.

По способу управления СКУД различают:

- автономные – для управления одним или несколькими устройствами преграждающими управляемыми (УПУ), без передачи информации на центральное устройство управления и без контроля со стороны оператора;
- централизованные (сетевые) – для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;
- универсальные (сетевые) – включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи.

По количеству контролируемых точек доступа:

- малой ёмкости (до 64 точек);
- средней ёмкости (от 64 до 256 точек);
- большой ёмкости (более 256 точек).

По функциональным характеристикам СКУД могут быть трёх классов:

1 - системы с ограниченными функциями;

2 - системы с расширенными функциями;

3 - многофункциональные системы.

Классификация средств и СКУД по устойчивости к несанкционированным действиям (далее НСД).

Классификация средств СКУД по устойчивости к НСД определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости:

- нормальной;
- повышенной;
- высокой.

УПУ классифицируют по устойчивости к разрушающим воздействиям.

Устойчивость УПУ устанавливается по:

- устойчивости к взлому;

- пулестойкости (только для УПУ со сплошным перекрытием проема);
- устойчивости к взрыву.

Нормальная устойчивость УПУ обеспечивается механической прочностью конструкции без оценки по показателям устойчивости к разрушающим воздействиям.

Для УПУ повышенной и высокой устойчивости со сплошным перекрытием проема (сплошные двери) и с блокированием объекта в проеме (шлюзы, кабины проходные) устанавливается классификация по устойчивости к взлому, взрыву и пулестойкости.

Устройства исполнительные (замки, защелки) классифицируют по устойчивости к разрушающим воздействиям в зависимости от конструкции.

По устойчивости к неразрушающим воздействиям средства СКУД в зависимости от их функционального назначения классифицируют по следующим показателям:

- устойчивости к вскрытию - для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивости к манипулированию;
- устойчивости к наблюдению для считывателей ввода запоминаемого кода (клавиатуры, кодовые переключатели и т.п);
- устойчивость к копированию (для идентификаторов);
- устойчивости защиты средств вычислительной техники (СВТ) средств управления СКУД от несанкционированного доступа к информации.

Классификация СКУД к НСД определяется для систем с централизованным управлением по защищенности от несанкционированного доступа к информации программного обеспечения СКУД и средств СВТ, входящих в состав сетевых СКУД.

3.2 Функции СКУД в составе систем противокриминальной защиты объектов.

СКУД применяются для предотвращения несанкционированного доступа людей, транспорта и других объектов в зону (из зоны) доступа (здания, помещения, территории, транспортные средства) в целях обеспечения противокриминальной защиты объектов.

СКУД действуют по принципу сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту, с информацией, заложенной в памяти системы.

СКУД должна выполнять следующие функции:

санкционирование – процедура присвоения каждому пользователю персонального идентификатора, кода, регистрацию его в системе (или регистрацию его биометрических признаков) и задание для него временных интервалов и уровня доступа (в какие помещения, когда и кто имеет право заходить);

идентификацию – процедуру опознавания пользователя по предъявленному идентификатору или биометрическому признаку;

авторизацию – проверку полномочий, заключающуюся в проверке соответствия времени и уровня доступа установленным в процессе санкционирования;

аутентификацию – установление подлинности пользователя по признакам идентификации;

разрешение доступа или отказ в доступе – выполняется на основании результатов анализа предыдущих процедур;

регистрация – протоколирование всех действий в системе;

реагирование – реакция системы на несанкционированные действия (подача предупреждающих и тревожных сигналов, отказ в доступе и т.д.)

3.3 Классификация СКУД.

1-й класс - системы с ограниченными функциями.

К СКУД 1-го класса относятся малофункциональные системы малой ёмкости, работающие в автономном режиме. Такие системы применяются в случае, если на объекте необходимо обеспечить контролируемый доступ сотрудников и посетителей, имеющих соответствующий идентификатор. При этом не ставится задача контроля времени доступа и выхода из помещения, регистрация проходов, передача данных на центральный компьютер.

Автономная система состоит из контроллера, обычно объединённого со считывателем, и исполнительного элемента. Как правило, используются магнитные (реже бесконтактные) карточки, электронные ключи "TouchMemory". В зависимости от типа контроллера количество лиц в списках может достигать от 60 до 2800 человек. Автономные системы снабжаются резервным питанием и имеют механический ключ для открывания замка в аварийных ситуациях.

Устанавливаются на объектах, где требуется только ограничение доступа посторонних лиц (функция замка).

2-й класс - системы с расширенными функциями.

СКУД 2-го класса – монофункциональные системы (одноуровневые и многоуровневые системы, работающие в автономном или сетевых режимах).

СКУД малой и средней емкости, но с возможностью расширения и включения их или их составных частей в общую линию связи (сетевой режим).

Данные системы имеют ряд дополнительных функций:

- ограничение допуска в охраняемую зону конкретного лица, группы лиц по дате и временным интервалам в соответствии с имеющимся идентификатором;
- автоматическую регистрацию событий в собственном буфере памяти, выдачу тревожных извещений (при несанкционированном проникновении, неправильном наборе кода или взломе

заграждающего устройства или его элементов) на внешние оповещатели или внутренний пост охраны;
- автоматическое управление открытием/закрытием устройства заграждения.

Устанавливаются на объектах, где требуется учёт и контроль присутствия сотрудников в разрешённой зоне, в качестве дополнения к имеющимся на объекте системам охраны и защиты.

На объектах, оборудованных средствами и системами охранно-пожарной сигнализации (ОПС), СКУД 2-го класса применяются как самостоятельные системы, и они часто рассматриваются только как средства усиления режима обеспечения безопасности объекта.

3-й класс – многофункциональные системы.

СКУД 3-го класса (сетевые). Контроллеры систем данного класса объединены в локальную сеть, работающую в реальном времени и ведущую непрерывный диалог с периферийными устройствами, с ведущим контроллером или с управляющим компьютером, расположенным в пункте охраны. Системы этих классов – крупные многоуровневые системы, рассчитанные на большое число пользователей (1500 человек и более).

Подобные системы применяются в случае, когда необходимо контролировать время прохода сотрудников и посетителей на объект и в помещения. При этом применяются более сложные электронные идентификаторы (Proximity, Виганд карточки, биометрический контроль или их сочетание). Время прохода на каждый день недели и для каждого владельца электронной карточки задаётся администратором системы.

Системы 3-го класса обычно интегрируются с системами охранно-пожарной сигнализации и системами телевизионного наблюдения на релейном уровне. Релейный уровень предполагает наличие дополнительного модуля в контроллере (или дополнительных входов/выходов в контроллере), к которому подключаются охранные или пожарные извещатели и релейные выходы для управления телекамерами и другими устройствами. Подобная интеграция применяется, в основном, на малых объектах. На таких объектах количество взаимодействий между системами невелико, и все они могут быть учтены в процессе проектирования системы безопасности. Этот уровень интеграции является простым, универсальным и достаточно надёжным.

3.4 Составляющие СКУД.

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

Турникет – устройство, устанавливаемое в проходах и предназначенное для создания физического барьера перед человеком до момента его

идентификации и последующего допуска его на территорию либо запрета допуска (Рисунок 1).



Рисунок 1. Турникет трипод.

Турникеты разделяются на:

- створчатые;
- роторные;
- триподные.
- Створчатые турникеты представляют собой управляемый физический барьер с системой створок, вращающихся с помощью электромоторов на вертикальных осях.

Створчатые турникеты могут оснащаться оптическими датчиками, служащими для обнаружения факта приближения к турникету. Также данные датчики служат для предотвращения несанкционированного прохода нескольких человек через один турникет (Рисунок 2).



Рисунок 2. Створчатый турникет.

Роторные турникеты представляют собой физический барьер с несколькими лопастями, закреплёнными на вращающейся вертикальной оси и встроенным электроприводом (Рисунок 3).



Рисунок 3. Роторный турникет.

Лопасти могут быть сплошными или изготавливаться из параллельно расположенных трубок. Различают полуростовые или полноростовые турникеты.

Полноростовые роторные турникеты полностью перекрывают зону прохода по высоте и используются как внутри помещений, так и снаружи на объектах, где требуется обеспечить повышенную безопасность (Рисунок 4).

Все приводы имеют блокировку обратного хода ротора, которая исключает обратное вращение при повороте ротора на определённый угол. Роторные турникеты имеют автоматическую разблокировку при получении сигнала от аварийной пожарной сигнализации.



Рисунок 4. Полноростовый роторный турникет.

Триподные турникеты представляют собой физический барьер в виде установленных на барабане трёх планок под углом к оси его вращения.

В исходном положении одна из планок параллельна поверхности земли и преграждает проход, в то время как две другие планки находятся в нижнем положении за пределами прохода (Рисунок 5).



Рисунок 5. Триподные турникеты.

Шлюзовая кабина – устройство, представляет собой металлическую конструкцию с автоматической системой сдвигающихся дверей, обеспечивающую защиту от несанкционированного проникновения в охраняемую зону, разделение людского потока (Рисунок 6).

Виды шлюзовых кабин:

- шлюзовые кабины с распашными дверями, оснащёнными различными типами устройств (доводчиками, электромагнитными замками, электромеханическими замками);
- шлюзовые кабины с автоматическими раздвижными дверями;
- шлюзовые кабины с автоматическими вращающимися створками.



Рисунок 6. Шлюзовая кабина.

Управление турникетами, шлюзами, проходными кабинами, дверями, воротами, шлагбаумами и противотаранными устройствами может осуществляться с брелока, с мобильного телефона, с использованием системы распознавания транспортного средства по радиометке, с использованием системы распознавания автомобильных номеров, централизованно с пульта СКУД.

Устройства исполнительные (УИ) – устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние устройств преграждающих управляемых (электромеханические, электромагнитные замки, электромагнитные защёлки, механизмы привода шлюзов, ворот, турникетов и другие подобные устройства).

Электромеханический принцип действия исполнительного механизма замка основан на перемещении закрывающих элементов (запоров, ригелей замков и т.п.) с помощью включения на время их передвижения электромотора или электромагнита (Рисунок 7).

В исполнительных механизмах с электромагнитным принципом действия отсутствуют движущиеся механические закрывающие элементы, то есть блокировка устройств заграждения (например, дверей) осуществляется с помощью сил магнитного притяжения, создаваемых мощным магнитом.

Часто в электромеханических замках применяют электромагнитную блокировку (магнитные защёлки, задвижки и т.п.) закрывающих элементов с возможностью перемещения их вручную при открывании или закрывании в экстремальных условиях.



Рисунок 7. Электромеханический замок.

Электромеханический замок рекомендуется устанавливать на деревянных и/или металлических дверях массой до 100 кг при условии средней нагруженности (100 – 200 проходов в день). Применение этого замка для дверей с высокой нагруженностью неэффективно из-за высокого механического износа и, как следствие, снижения надёжности и срока службы. Чаще всего электромеханический замок устанавливают на двери (накладной или врезной замок), но иногда его устанавливают и на дверной коробке.

Электромагнитный замок (Рисунок 8) рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг при условии высокой нагруженности (более 200 проходов в день). Отсутствие деталей, подверженных трению и износу, делает этот замок практически вечным.

Особенностью данного замка является необходимость постоянной подачи тока на обмотку электромагнита, при пропадании напряжения в сети (например, при аварии или умышленном обрыве проводов) замок открывается. В связи с этим для надёжной работы необходимо дублировать электромагнитный замок механическим или применять дополнительное резервное питание.

Электромагнитную защёлку рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери (при ее закрывании), и разблокировать замок при подаче сигнала управления на открывание двери. Такая установка защёлки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромагнитные замки с плоским якорем выпускают двух видов: с якорем, работающим на отрыв, и с якорем, работающим на сдвиг. В обесточенном состоянии все замки нормально открыты. Замки с якорем "на отрыв" изготавливают в накладном варианте, а с якорем "на сдвиг" – в накладном и врезном вариантах.

Для входных дверей используют электромагнитные замки с силой удержания от 200 до 600 кг, при этом ток потребления таких замков (при напряжении питания 12 В) составляет от 200 до 500 мА.

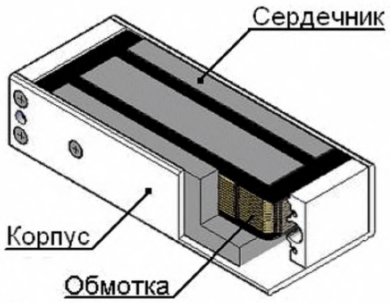


Рисунок 8. Электромагнитный замок.

Помимо прямоугольных электромагнитных замков освоен выпуск круглых замков. Это позволило упростить изготовление и снизить стоимость. К недостаткам электромагнитных замков следует отнести потерю работоспособности при образовании зазора между электромагнитом и пластиной. Во избежание такой ситуации пластину укрепляют на резиновой прокладке, компенсирующей образующийся зазор.

Требование обеспечения соприкосновения электромагнита и пластины без зазора для обеспечения работоспособности замка, вызывает

необходимость обязательного применения качественного дверного доводчика.

Функция доводчика – не только гарантировать закрытие двери, но также оберегать замок от механических ударов.

Электромагнитные замки с плоским якорем имеют очень высокую надёжность, это определяется, в основном, конструкцией замка и в значительной степени – отсутствием трущихся деталей, износ которых ограничивает долговечность. Ударные нагрузки, возникающие при закрывании двери (особенно, если дверной доводчик плохо отрегулирован), и перепады температуры создают тяжёлые условия для элементов электроники. Поэтому их размещают вне корпуса замка.

Устройства считывающие (УС).

УС – это устройство, предназначенное для считывания (ввода) идентификационных признаков с целью опознания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. По принципу считывания они могут быть:

- с ручным вводом;
- контактные;
- бесконтактные;
- биометрические;
- комбинированные.

Идентификаторы (ИД) (носитель идентификационного признака).

Идентификатор – это уникальный признак субъекта или объекта. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код – предмет, в котором (на который) с помощью специальной технологии занесён идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и другие устройства).

Разновидности идентификаторов.

Механические – представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей).

К механическим идентификаторам относятся такие устройства, как кодовые панели и механические ключи. Механические идентификаторы просты и имеют несколько недостатков: простота подделки, наличие движущихся частей, которые снижают надёжность, невозможность использования для идентификации личности.

Магнитные – представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда) (Рисунок 9).



Рисунок 9. Карта доступа с магнитной полосой.

Данная технология получила широкое распространение в системах контроля и управления доступом благодаря относительной сложности подделки идентификаторов, возможности применения карт в качестве идентификаторов личности. Магнитные системы позволяют разграничивать доступ для большого числа пользователей (до 2000 и более).

Оптические – представляют собой нанесённые на поверхность или внутри идентификатора метки, имеющие различные оптические характеристики (карты со штрих кодом, голографические метки) (Рисунок 10).



Рисунок 10. Карта доступа со штрих кодом.

Электронные контактные – представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи) (Рисунок 11).



Рисунок 11. Электронная карта доступа.

Электронный ключ TouchMemory представляет собой металлическую "таблетку" небольшого диаметра толщиной 4-6 мм, внутри которой запрессована электронная микросхема с уникальным 48-разрядным кодом. "Таблетка" не имеет собственного источника питания, а заряжается от считывателя при соприкосновении с ним. И ключ, и считыватель изготавливаются в герметичном исполнении, что делает их практически вечными. Они надёжны в работе, имеют высокую устойчивость к электромагнитным и криминальным воздействиям. Для удобства пользования "таблетка" закрепляется в пластмассовой пластинке, имеющей отверстие для подвешивания её на одну связку с другими ключами (Рисунок 12).



Рисунок 12. Электронные ключи TouchMemory.

Карточка бесконтактная (Proximity) – карточка, с которой информация о коде ключа считывается радиочастотным способом на расстоянии (то есть без непосредственного контакта со считывателем). Различают пассивные и активные карточки. Пассивные карточки питаются энергией, получаемой от считывателя, и действуют на расстоянии до 10 см (Рисунок 13).



Рисунок 13. Карточка бесконтактная (Proximity).

Активные – имеют встроенную батарейку, срок работы которой составляет до 10 лет. Считыватель размещается, как правило, скрытно в полости неметаллической двери или за радиопрозрачной стенкой. В пассивных карточках информация записывается один раз на всё время действия карточки, а в активных существует возможность ее изменения.

Электронные радиочастотные – считывание кода с электронных идентификаторов происходит путём передачи данных по радиоканалу.

Акустические – представляют собой кодированный акустический сигнал.

Биометрические считыватели (только для считывания) представляют собой индивидуальные признаки человека (отпечатки пальцев, геометрию ладони, рисунок сетчатки глаза, динамику подписи) (Рисунок 14).



Рисунок 14. Биометрический считыватель.

При идентификации по индивидуальным биометрическим признакам определяется именно человек – носитель этих признаков, а не выданный ему документ – карта, код, ключ и т.п. Это является основным отличием данных систем от любых других идентифицирующих устройств. Самые распространённые признаки человека, которые используются для биометрической идентификации:

- отпечатки пальцев;
- узор кровеносных сосудов сетчатки глаза;
- геометрия кисти;
- изображение лица;
- динамика подписи;
- голосовые характеристики.

Идентификация по индивидуальным биометрическим признакам позволяет использовать эти устройства в системах контроля доступа на особо важных объектах: военных базах; правительственных учреждениях; хранилищах банков; компьютерных центрах. Там, где самым важным требованием является секретность, а остальные требования: по пропускной способности, по стоимости, по удобству пользования, – имеют второстепенное значение.

Комбинированные – для идентификации используют одновременно несколько идентификационных признаков.

Средства управления (аппаратные устройства).

Контроллер доступа (КД) и прибор приемно-контрольный доступа (ППКД) представляют собой аппаратное устройство в составе средств управления системы контроля и управления доступом (Рисунок 15).

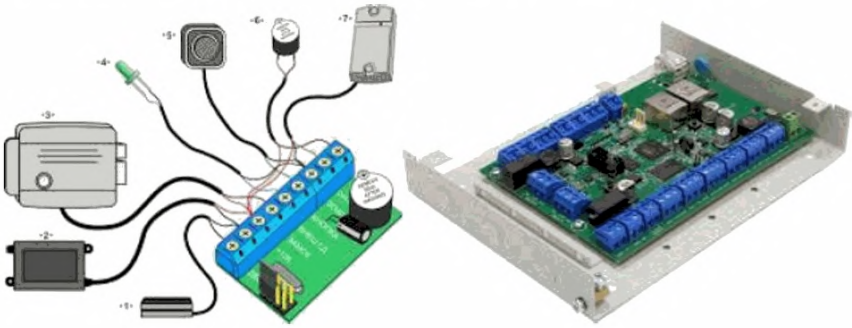


Рисунок 15. Контроллер доступа.

Автономный – для управления одним или несколькими устройствами преграждающими управляемыми без передачи информации на центральное устройство управления и контроля со стороны оператора.

Централизованный (сетевой) – для управления устройствами преграждающими управляемыми с обменом информацией с центральным пультом и контролем управления системой со стороны центрального устройства управления.

Универсальный (сетевой) – включает в себя функции как автономных, так и сетевых систем, работающих в сетевом режиме под управлением центрального устройства управления, переходящий в автономный режим при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи.

Домофоны.

Домофон – устройство для управления доступом с возможностью дистанционного управления сотрудником дежурной смены на основе получаемой аудио/видеоинформации (Рисунок 19).

Домофоны сочетают в себе функции аудио- и/или видеоконтроля и управления доступом на объекте. Домофоны позволяют абоненту, не подходя к двери, идентифицировать посетителя по изображению и/или голосу и дистанционно управлять входной дверью.

Домофон позволяет, соблюдая безопасную дистанцию между посетителем и охраной объекта, выяснить требующуюся информацию о посетителе и принять взвешенное решение о его допуске на объект.

При выборе домофона необходимо обращать особое внимание на его климатическое исполнение, антивандальные свойства, надёжность.



Рисунок 19. Домофоны.

По виду (способу идентификации посетителей) домофоны подразделяются на:

Аудиодомофоны (Рисунок 20) обеспечивают двухстороннюю аудиосвязь абонента с посетителем и позволяют идентифицировать посетителя по его голосу.



Рисунок 20. Схема оборудования входа аудиодомофоном.

Видеодомофоны (Рисунок 21) обеспечивают видеоконтроль наружного околодверного пространства, двухстороннюю аудиосвязь абонента с посетителем и позволяют идентифицировать посетителя по его изображению и голосу.



Рисунок 21. Схема оборудования входа видеодомофоном.

По количеству обслуживаемых абонентов различают:

Индивидуальные (одноабонентские) – домофоны позволяют обслуживать только одного абонента и применяют для защиты отдельных квартир, небольших офисов, загородных домов, а также могут быть установлены на постах охраны.

Видеодомофон обеспечивает более высокий уровень безопасности абонента, чем аудиодомофон, так как (помимо двухсторонней аудиосвязи) позволяет получить телевизионное изображение посетителя.

При выборе домофона следует обращать особое внимание на такие факторы:

- климатическая устойчивость, прежде всего – диапазон рабочих температур, который должен быть для некоторых блоков (например, блока вызова, электрозамка, доводчика двери) не менее минус 40÷плюс 40° С;
- устойчивость к вандализму;
- устойчивость к нестабильному электропитанию;
- наличие сертификата соответствия;
- обязательное наличие полной эксплуатационной документации с принципиальными и монтажными схемами на русском языке;
- наличие стабильного гарантийного и послегарантийного обслуживания предлагаемого оборудования и возможность закупки ремонтных ЗИП.

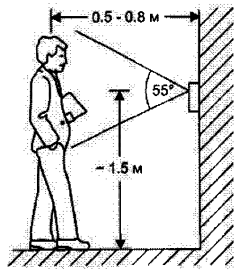


Рисунок 22. Рекомендуемая высота установки видеодомофона.

3.5 Электропитание СКУД.

Основное электропитание СКУД должно осуществляться от сети переменного тока частотой 50 Гц номинальным напряжением 220 В.

СКУД должна быть работоспособна при допустимых отклонениях напряжения сети от минус 15% до плюс 10%.

Электропитание отдельных средств СКУД допускается осуществлять от других источников с иными параметрами выходных напряжений, требования к которым устанавливают в нормативных документах на СКУД конкретных типов.

СКУД должны быть обеспечены резервным электропитанием при пропадании напряжения основного источника электропитания.

В качестве резервного источника электропитания может использоваться резервная сеть переменного тока или источники постоянного тока.

Переход на резервное электропитание должен осуществляться автоматически без нарушения установленных режимов работы и функционального состояния средств СКУД.

Резервный источник электропитания должен обеспечивать выполнение основных функций системы при пропадании напряжения в сети:

Системы 1 класса – 0,5 ч.

Системы 2 класса – 0,5 ч.

Система 3 класса – 1 ч.

Допускается не применять резервирование электропитания с помощью аккумуляторных батарей для УПУ, которые требуют для управления значительных мощностей приводных механизмов (приводы ворот, шлюзы).

При этом такие УПУ должны быть оборудованы аварийными механическими средствами открывания и системными средствами индикации аварии электропитания.

При использовании в качестве источника резервного электропитания СКУД аккумуляторных или сухих батарей рекомендуется иметь индикацию разряда батареи ниже допустимого предела.

Химические источники электропитания, встроенные индикаторы или обеспечивающие сохранность данных в контроллерах, должны обеспечивать работоспособность СКУД в течение не менее трёх лет.

3.6 Выбор СКУД для оборудования объекта.

Выбор варианта оборудования объекта средствами СКУД следует начинать с его обследования.

Целью обследования является определение размера возможного ущерба предприятию (организации) или собственнику имущества и связанной с ним категории объекта.

По результатам обследования определяются тактические характеристики и структура СКУД, а также составляется техническое задание на оборудование объекта СКУД. В техническом задании указывается:

- назначение СКУД, техническое обоснование и описание системы;
- размещение составных частей системы;
- условия эксплуатации средств СКУД;
- основные технические характеристики.

Основные технические характеристики:

- пропускная способность в охраняемые зоны, особенно в час-пик;
- максимально возможное число пользователей на один считыватель;
- максимальное число и виды идентификаторов;
- требования к маскировке и защите средств СКУД от вандализма;
- оповещение о тревожных и аварийных ситуациях и принятие соответствующих мер по их пресечению или предупреждению;
- возможность работы и сохранения данных без компьютера или при его отказе;
- алгоритм работы системы СКУД в аварийных и чрезвычайных ситуациях;
- программное обеспечение системы;
- требования к безопасности;
- требования к электропитанию;
- обслуживание и ремонт системы;
- требования к возможности включения системы СКУД в интегрированную систему безопасности.

Путём изучения чертежей, обхода и осмотра объекта, а также проведения необходимых измерений определяются:

- количество входов/выходов и их геометрические размеры (площадь, линейные размеры, пропускная способность и т.п.);
- материал строительных конструкций;

- количество отдельно стоящих зданий, их этажность;
- количество открытых площадок;
- количество отапливаемых и неотапливаемых помещений и их расположение.

Учитывать вредное воздействие окружающей среды следует лишь для исполнительных устройств, считывателей и контроллеров (совмещенных со считывателями в одном конструктивном блоке), предназначенных для работы вне отапливаемых закрытых помещений либо в особых условиях (запылённость, повышенная влажность, отрицательная температура, агрессивная среда и т. п.). Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, удалённость считывателей и контроллеров от управляющего центра, заземление составных частей системы и т.п.

3.7 Размещение и монтаж СКУД.

Устройства центрального управления.

Устройства центрального управления (персональные компьютеры), являющиеся "мозгом" СКУД, рекомендуется устанавливать в отдельных служебных помещениях, защищённых от доступа посторонних лиц, например, в помещении дежурной части.

Основные положения, в соответствии с которыми разрабатываются режимы работы всей системы безопасности, определяются руководящим составом объекта, исходя из общей концепции обеспечения безопасности объекта. Управляющие программы загружаются в центральный управляющий и вспомогательные компьютеры или контроллеры и защищаются секретными кодами.

Персонал охраны, а также других служб, которые подключены к общей компьютерной сети, не должны иметь доступа к программным средствам и возможности влиять на установленные режимы работы, за исключением лиц, ответственных за данные работы.

При объединении компьютеров в сеть целесообразно разделять функциональные возможности среди пользователей сети и в соответствии с этим размещать компьютеры в помещениях объекта.

Устройства контроля и управления.

Ведущие контроллеры и контроллеры, работающие на несколько устройств заграждения, рекомендуется размещать в специальных запираемых металлических шкафах или нишах, на высоте, удобной для технического обслуживания. При этом следует дверцы данных шкафов или ниш блокировать охранной сигнализацией на возможное открытие или пролом.

Корпус данных контроллеров должен быть выполнен из ударопрочного материала, защищающего контроллер от актов вандализма. Контроллеры, управляющие работой считывателей или исполнительных устройств одной

двери в двух направлениях, рекомендуется устанавливать с внутренней стороны охраняемого помещения.

При работе устройств контроля и управления в сетевом режиме необходимо учитывать возможность появления помех и сбоев в работе из-за неправильного монтажа соединительных линий и их длины.

Для нормальной работы рекомендуется:

- при значительной длине соединительного кабеля подключать к шине оконечные и согласующие элементы. Необходимое точное значение величины этих элементов зависит от характеристик кабеля;
- заземлять устройства и экранированные оплётки кабелей в одной точке (во избежание возникновения блуждающих токов), желательно у ведущего контроллера. При большой длине кабелей заземление можно производить в разных точках, но при этом обязательно использовать специальные методы и устройства защиты от помех;
- использовать шинные усилители при большой длине кабеля.

Считыватели и устройства исполнительные.

В зависимости от типа считывателей и устройств исполнительных, пропускной способности и организации системы безопасности объекта в целом, они могут устанавливаться как вблизи устройств заграждения, так и непосредственно на них. При их размещении необходимо учитывать условия эксплуатации, удобство монтажа, надёжность и вандалостойкость.

Считыватели "Proximity" удобнее всего размещать на стене, скрытно в стене перед устройствами заграждения или с внутренней стороны устройства заграждения, например, на внутренней стороне неметаллической двери, если её толщина не превышает 10 см.

При монтаже считывателя на металле рекомендуется, чтобы между основанием считывателя и металлической поверхностью расстояние было не менее 25 мм. В случае, когда стена, за которой установлен считыватель, оказывается слишком толстой или изготовлена из металла (содержит металлическую арматуру), считыватель допускается устанавливать на расстоянии, на котором должна быть обеспечена необходимая защита от возможного несанкционированного прохода.

Считыватели магнитных, Виганд карточек, электронных ключей и клавиатуры также рекомендуется размещать на стене или непосредственно на устройстве заграждения на высоте, удобной для пользования.

Считыватели магнитных карточек (за исключением совмещённых с исполнительными устройствами) во избежание помех или даже выхода из строя не рекомендуется устанавливать в непосредственной близости от мощных исполнительных устройств, создающих сильные электромагнитные поля (соленоидные, магнитные замки и т.п.).

Электромагнитные защёлки рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка,

установленного в двери, при закрывании двери и разблокировать замок при подаче сигнала от контроллера. Кроме того, такая установка защёлки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромеханические замки рекомендуется устанавливать на деревянных и металлических дверях массой до 100 кг при условии средней загруженности (до 100 – 200 проходов в день). Применение этих замков для дверей с высокой загруженностью неэффективно по причине высокого механического износа и как следствие снижения надёжности и срока службы. Чаще всего электромеханические замки устанавливают на двери (накладной или врезной замок), но иногда эти замки устанавливаются и на дверной коробке.

Электромагнитные замки рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг в условиях высокой загруженности (более 200 проходов в день). Отсутствие деталей, подверженных трению и износу, делает этот замок практически вечным. Особенностью данного замка является необходимость постоянной подачи тока на обмотку его электромагнита, так как при пропадании напряжения питания, например, при аварии или умышленном обрыве проводов, замок открывается. В связи с этим для надёжной работы необходимо дублирование его механическим замком или применение дополнительного резервного электропитания.

При совместном использовании магнитоконтактных извещателей в качестве датчиков положения двери с электромагнитными и электромеханическими замками, они должны быть разнесены друг от друга как можно дальше.

При установке исполнительных устройств (замки, доводчики, приводы и т.п.), требующих для своей работы подводки электропитания, необходимо использовать специальные устройства и кабели, обеспечивающие электро- и пожаробезопасность (особенно на сгораемых конструкциях), а также защиту от повреждений при открытии/закрытии дверей (гибкие переходы).

3.8 Общие требования к минимально необходимому составу СКУД.

3.8.1 Минимально необходимый состав СКУД.

Объекты органов внутренних дел Российской Федерации, отнесённые к II категории, должны быть оборудованы СКУД.

СКУД оборудуются:

- проходные;
- служебные помещения;
- специальные помещения.

Проходная в здание оборудуется СКУД (см. приложение 2, 4):

- вход в здание;
- вход в помещение дежурной части.

Внутри здания СКУД оборудуются (см. приложение 2-7):

- служебные помещения;
- специальные помещения.

3.8.2 Технические требования к СКУД.

СКУД должна обеспечивать:

- контроль и управление точками доступа (двери, турникеты, ворота) на вход и выход;
- подключение считывателей электронных кодовых ключей;
- контроль аварийного открывания преграждающих устройств;
- контроль блокировки преграждающих устройств;
- контроль отказа от прохода;
- контроль исправности запорного устройства;
- возможность передачи тревожной информации на автоматизированные рабочие места системы сбора и обработки информации;
- контроль состояния связи с контроллерами системы контроля и управления доступом;
- защиту цепей питания от перенапряжения, переполюсовки и перегрузок;
- защиту входных цепей от перенапряжения и переполюсовки;
- дистанционное управление (блокирование, разблокирование);
- автономную работу без потери данных в течение не менее 24 ч. при потере связи с автоматизированными рабочими местами;
- глобальный контроль повторного прохода;
- зональный контроль местоположения персонала;
- дуплексную речевую связь с оператором с регистрацией в аудиоархиве;
- фотоидентификацию (вывод на монитор фотографий из базы данных) проходящих через точку доступа;
- ведение базы данных персонала;
- ведение журнала событий;
- получение отчёта о проходах;
- работу бюро пропусков;
- возможность наращивания количества устройств в процессе эксплуатации;
- получение информации о нахождении сотрудников (работников) на территории, времени их прихода или ухода, формирование списка всех сотрудников (работников), находящихся на территории;
- вывод на монитор текстовой информации о входящем (выходящем);
- идентификация (получение разрешения на проход, проезд) должна осуществляться по двум и более признакам.

Средства управления доступом могут быть функционально интегрированы со средствами обнаружения запрещённых к проносу предметов и материалов.

При срабатывании средств обнаружения запрещённых к проносу (провозу) предметов (материалов) должны подаваться сигналы оповещения

сотрудников, а также сигналы управления запирающими устройствами преграждающих конструкций (турникетов, дверей).

Эвакуационные и аварийные выходы должны быть оборудованы устройством экстренного открывания дверей (устройство «Антипаника») по ГОСТ 31471-2011 «Устройства экстренного открывания дверей эвакуационных и аварийных выходов. Технические условия».

«Антипаниковая» дверь – это металлическая дверь, устойчивая к взлому снаружи и оборудованная специальными «антипаниковыми» замками и извещателем на открывание с выводом на КПП.

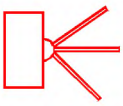
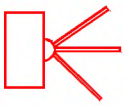
Примечания:

Аттестованные помещения, а также помещения, предназначенные для обработки сведений, составляющих государственную тайну, оборудуются техническими средствами ОС, прошедшими сертификацию по стандартам ФСТЭК России и ФСБ России.

ПРИЛОЖЕНИЯ

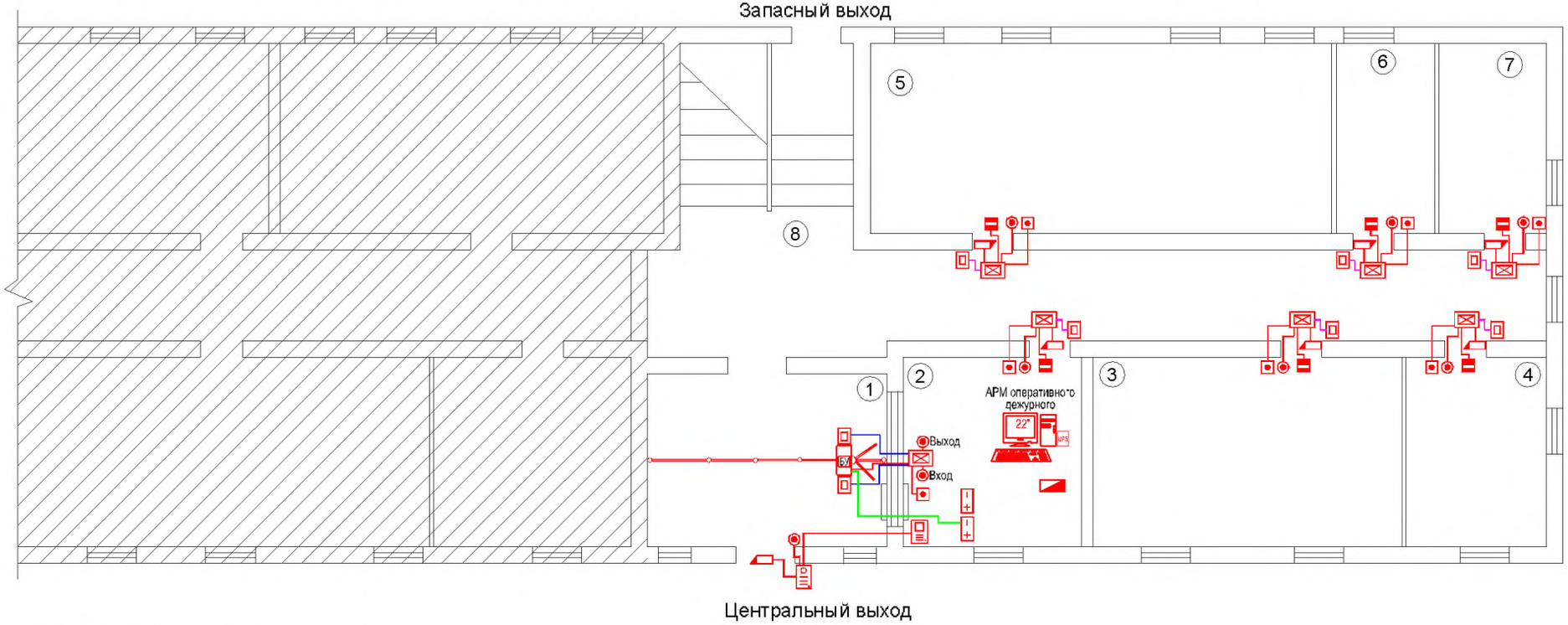
Приложение 1

Условные обозначения

Наименование	Обозначение	
	на планах	на схемах
Холл АРМ дежурного оператора		
Пульт управления		
Контроллер управления доступом		
Бесконтактный считыватель с клавиатурой		
Извещатель охранный магнитоконтактный		
Кнопка "ВЫХОД"		
Кнопка аварийного разблокировки электромагнитного замка (турникета)		
Электромагнитный замок		
Монитор видеодомофона		
Вызывная панель видеодомофона		
Турникет		
Резервированный источник электропитания питания 12В		
Бесперебойный источник питания		
Блок управления турникетом		
Провод КПСВВнг(А)FRLS1х2х0,5		
Провод КПСВВнг(А)FRLS1х2х1,5		
Провод КПСВЭВнг(А)FRLS2х2х1,5		
Провод UTP4х2х0,5		

Приложение 2

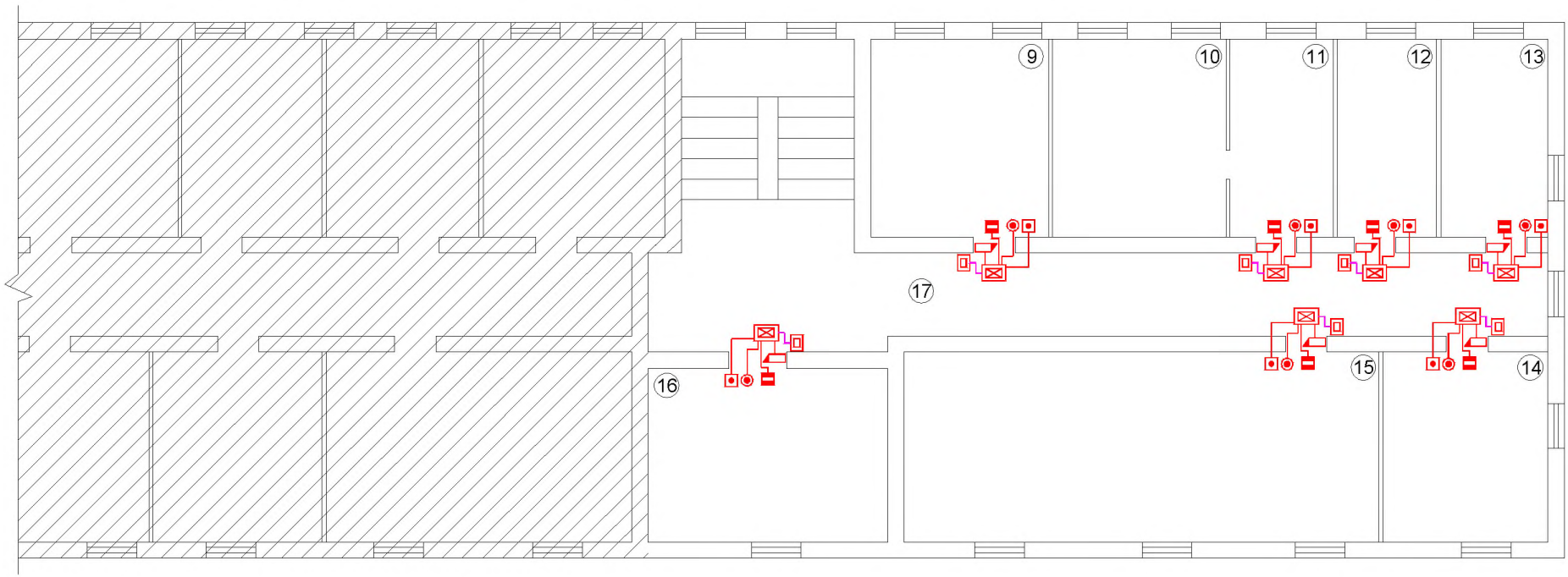
План расположения оборудования СКУД 1-го этажа ОВД



№ п/п	Наименование
1	Холл
2	Помещение охраны
3	Архив
4	Кабинет
5	Секретариат
6	Кабинет
7	Сан.узел
8	Коридор

План расположения оборудования СКУД 2-го этажа ОВД

Приложение 3



№ п/п	Наименование
9	Юристконсульт
10	Кабинет начальника
11	Приемная
12	Кабинет
13	Спецпомещение
14	Кабинет
15	Учебный класс
16	Группа кадров
17	Коридор

Приложение 4

План расположения оборудования СКУД 1-го этажа ЛОВД



№ п/п	Наименование
101	Зал оперативного дежурного
102	Комната хранения оружия
103	Комната чистки оружия
104	Комната для хранения средств защиты, связи, оперативной и криминальной техники
105	Аппаратная
106-108	Специальное помещение для содержания задержанных лиц
109	Сан.узел
110	Комната следственно-оперативной группы
111	Помещение для выявления обстаятельств задержания или доставление лиц, доставленных в дежурную часть

112	Помещение для размещения конвоя
113	Комната для подогрева и приема пищи
114	Коридор
115	Холл
116	Серверная
117	Кабинет
118	Кабинет
119	Сан.узел
120	Комната старшины
121	Кабинет
122	Кабинет
123	Коридор

Приложение 5

План расположения оборудования СКУД 2-го этажа ЛОВД



№ п/п	Наименование
201	Сан.узел
202	Кабинет
203	Кабинет
204	Кабинет
205	Секретариат
206	Кабинет
207	Коридор
208	Кабинет
209	Коридор
210	Архив
211	ОДиР
212	ОДиР

213	Кабинет оперативного направления
	и мобилизационной готовности
214	Сан.узел
215	Кладовая хранения вещественных
	доказательств
216	Кладовая экспертно-
	криминалистического отдела
217	Кабинет оперуполномоченного
	секретной части
218	Кабинет
219	Кабинет
220	Коридор
221	Коридор

Приложение 6

План расположения оборудования СКУД 3-го этажа ЛОВД

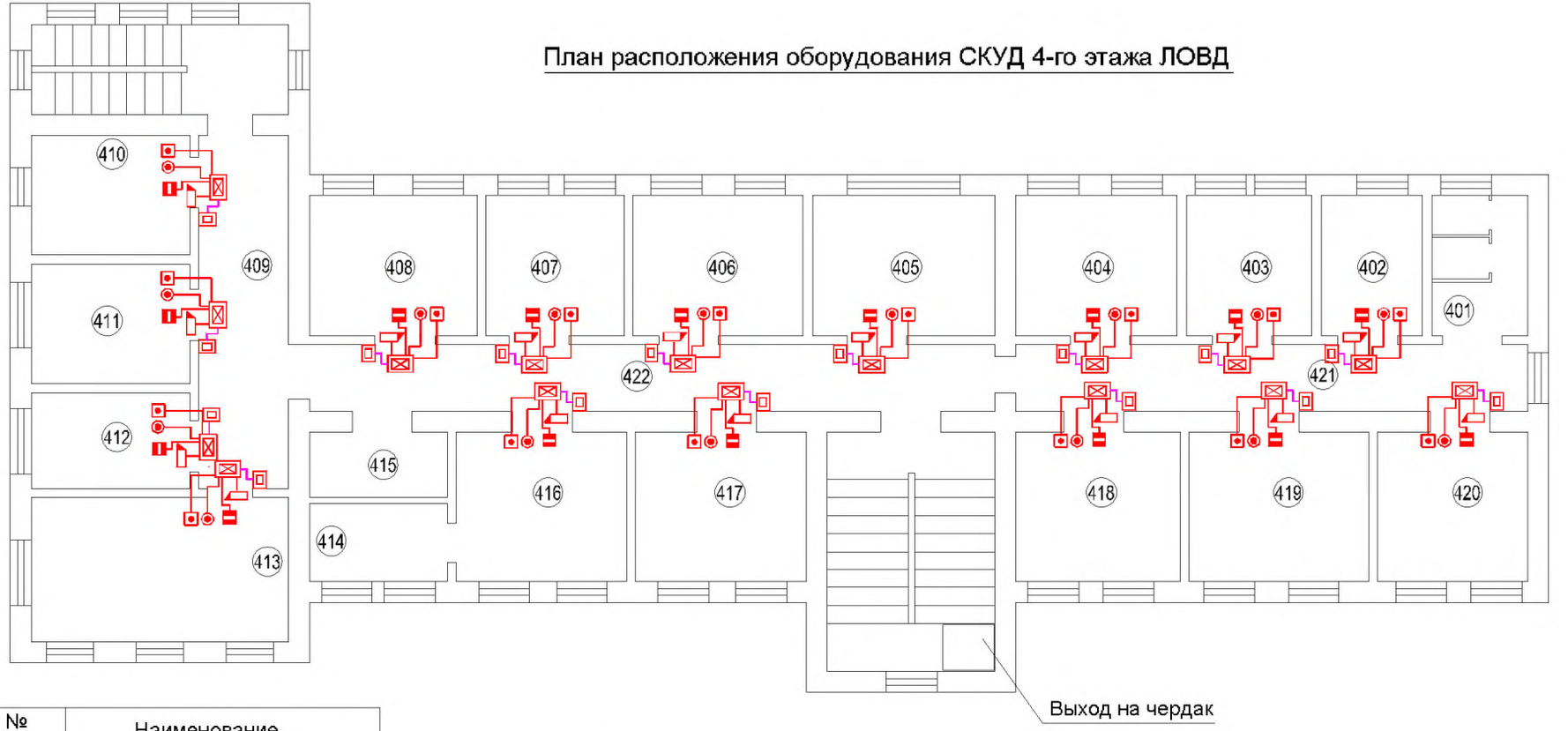


№ п/п	Наименование
301	Кабинет
302	Секретка (спецпомещение)
303	Холл
304	ФЭО
305	ФЭО
306	Кабинет
307	Актовый зал

308	Сан.узел
309	Касса
310	Кабинет
311,312	Экспертно-криминалистический
	отдел
313	Кабинет
314	Коридор
315	Коридор

Приложение 7

План расположения оборудования СКУД 4-го этажа ЛОВД

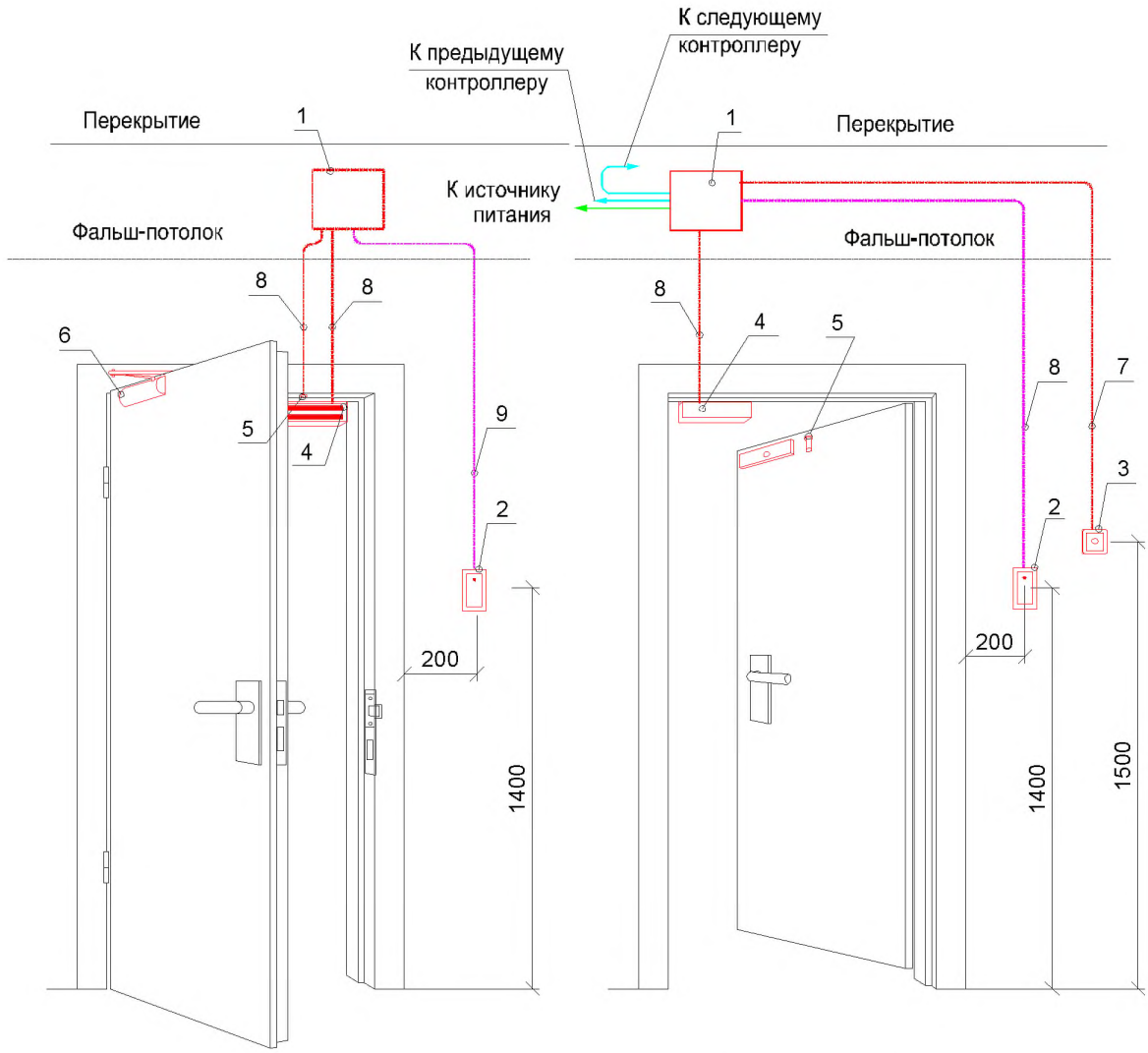


№ п/п	Наименование
401	Сан.узел
402	Кабинет
403	Кабинет
404	Кабинет
405	Кабинет
406	Кабинет
407	Кабинет
408	Кабинет
409	Коридор
410	Отдел кадров
411	Отдел кадров

412	Кабинет
413	Архив
414	Комната отдыха
415	Туалет
416	Кабинет начальника
417	Приемная
418	Кабинет
419	Кабинет
420	Кабинет
421	Коридор
422	Коридор

Приложение 8

Схемы установки средств СКУД на одностворчатой двери



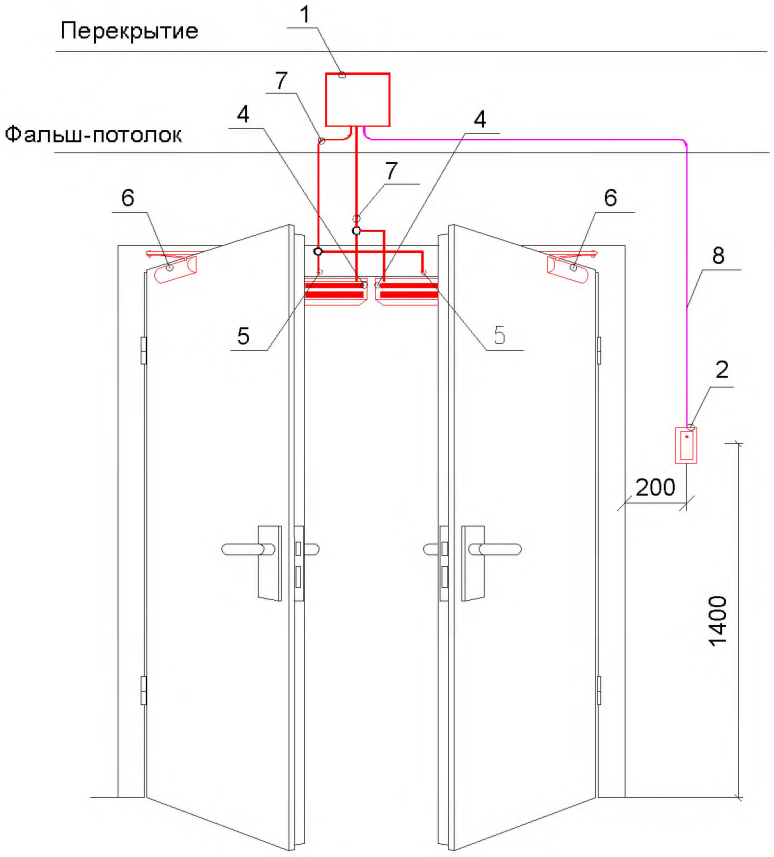
Вид со стороны коридора

Вид со стороны защищаемого помещения

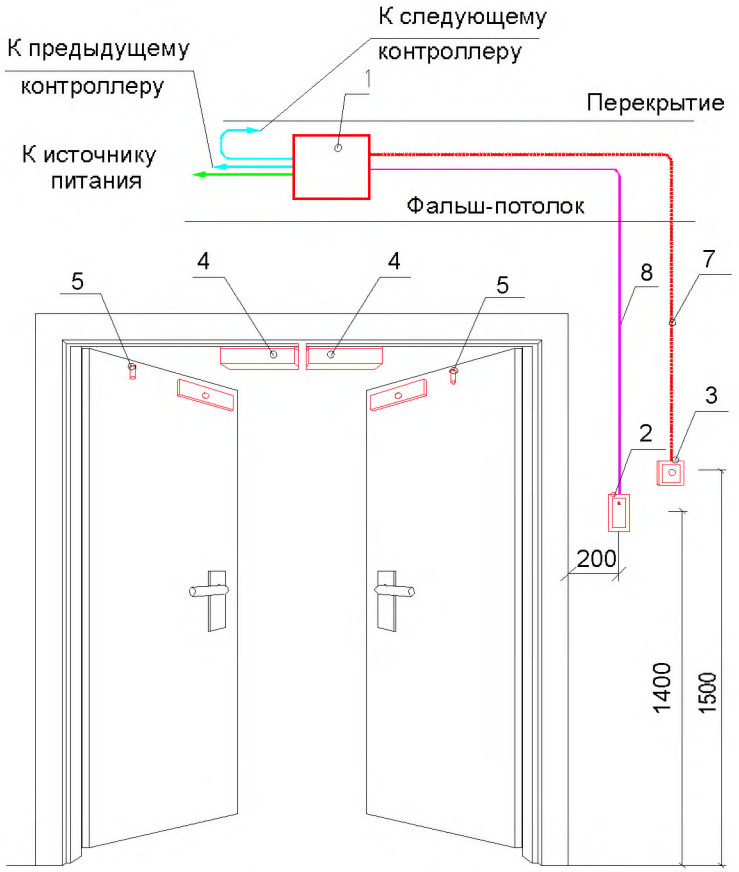
№ п/п	Наименование
1	Контроллер управления доступом
2	Бесконтактный считыватель с клавиатурой
3	Кнопка аварийной разблокировки электромагнитного замка
4	Электромагнитный замок
5	Извещатель охранный магнитоконтактный
6	Доводчик дверной
7	Провод
8	Провод

Приложение 9

Схемы установки средств СКУД на двустворчатой двери



Вид со стороны коридора



Вид со стороны защищаемого помещения

№ п/п	Наименование	№ п/п	Наименование
1	Контроллер управления доступом	5	Извещатель охранный магнитоконтактный
2	Бесконтактный считыватель с клавиатурой	6	Доводчик дверной
3	Кнопка аварийной разблокировки электромагнитного замка	7	Провод
4	Электромагнитный замок	8	Провод

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к третьей категории»

Москва 2016 г.

СОДЕРЖАНИЕ

№ раздела	Наименование системы	№ листов
1	Система охранно-тревожной сигнализации.	3-56
2	Система охранной сигнализации внешнего периметра объекта	57-109
3	Система охранная телевизионная.	110-145
4	Система контроля и управления доступом.	146-174

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к третьей категории»

Система охранно-тревожной сигнализации

РАЗДЕЛ 1

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	6
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	8
3.	СИСТЕМА ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ (СОТС)	9
3.1	Назначение СОТС	9
3.2	Состав СОТС	9
3.3	Средства обнаружения проникновения	9
3.4	Критерии выбора СОТС	27
3.5	Организация передачи информации на пульт централизованного наблюдения (ПЦН)	28
3.6	Электропитание	29
3.7	Общие требования к минимально необходимому составу СОТС	31

ПРИЛОЖЕНИЯ

Приложение 1.	Условные обозначения.	35
Приложение 2.	Схема блокировки двери, окна извещателем охранным магнитоконтактным.	36
Приложение 3.	Схема установки извещателя охранного ударноконтактного для блокировки окна.	37
Приложение 4.	Схема установки извещателя охранного поверхностного звукового (акустического).	38
Приложение 5.	Схема установки извещателя охранного поверхностного оптико-электронного (инфракрасного).	39
Приложение 6.	Схема установки извещателя охранного объёмного ультразвукового.	40
Приложение 7.	Схема установки извещателя охранного объёмного радиоволнового.	41
Приложение 8.	Схема установки извещателя охранного объёмного оптико-электронного (инфракрасного).	42
Приложение 9.	Схема установки извещателя охранного поверхностного вибрационного на стене.	43
Приложение 10.	Схема установки извещателя охранного поверхностного вибрационного с датчиком наклона.	44
Приложение 11.	Схема установки извещателя охранного поверхностного вибрационного для охраны немонолитной (многосекционной) конструкции.	45
Приложение 12.	Схема установки извещателя охранного объёмного совмещённого (ИК+АК).	46

Приложение 13.	Схема установки извещателя охранного поверхностного совмещённого (ИК+АК).	47
Приложение 14.	Схема блокировки венткороба омическим извещателем.	48
Приложение 15.	Схема блокировки окна омическим извещателем.	49
Приложение 16.	План расположения оборудования СОТС УВО.	50
Приложение 17.	План расположения оборудования СОТС 1-го этажа здания гаража. Оси 1-11.	51
Приложение 18.	План расположения оборудования СОТС 1-го этажа здания гаража. Оси 11-22.	52
Приложение 19.	План расположения оборудования СОТС 2-го этажа здания гаража. Оси 1-13/1.	53
Приложение 20.	План расположения оборудования СОТС 2-го этажа здания гаража. Оси 13/1-22.	54
Приложение 21.	План расположения оборудования СОТС 1-го этажа здания ОВД.	55
Приложение 22.	План расположения оборудования СОТС 2-го этажа здания ОВД.	56

1. ОБЩАЯ ЧАСТЬ

Методические рекомендации по оснащению ведомственных объектов СОТС разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 02.01.2013 № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;

- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- ГОСТ Р 50658-94 (МЭК 60839-2-4:1990) «Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений»;
- ГОСТ Р 50659-12 «Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний»;
- ГОСТ Р 50777-14 «Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок Общие технические требования и методы испытаний»;
- ГОСТ Р 51186-98 «Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний»;
- Р 78.36.018–2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- Р 78.36.019–2012 «Рекомендации по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий»;
- Р 78.36.026-2012 «Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны ограждённых территорий и открытых площадок»;
- Р 78.36.028-2012 «Рекомендации. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов»;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану. Методические рекомендации»;
- Р 78.36.032-2013 «Инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1.»

- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения;
- Р 78.36.050-2015 «Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних периметров, дверей, окон, витрин и подступов к отдельным предметам»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

В соответствии с пунктом 4.3 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом III категории по степени потенциальной угрозы понимается отдельно стоящие здания или сооружения, имеющие прилегающую территорию (или без таковой), на которых осуществление круглосуточного пропускного режима и круглосуточного дежурства не обязательно.

3. СИСТЕМА ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ

3.1 Назначение системы охранно-тревожной сигнализации.

СОТС – это 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.

СОТС является основой построения системы безопасности объекта.

В основе построения СОТС и организации ее функционирования лежит принцип создания последовательных рубежей охраны.

При выборе технических средств охраны для оборудования объекта СОТС рекомендуется применять приборы, указанные в «Списке технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для

применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (действующая редакция).

3.2 Состав СОТС.

СОТС включает в себя:

- средства обнаружения проникновения (охранные извещатели);
- средства тревожной сигнализации (СТС);
- приборы приемно-контрольные (ППК), и охранно-пожарные (ППКОП), устройство оконечное объектовое (УОО) системы передачи извещений (СПИ);
- средства оповещения (оповещатели световые, звуковые, комбинированные светозвуковые);
- СПИ на пульт централизованного наблюдения (ПЦН);
- источники вторичного электропитания (ИВЭП).

3.3 Средства обнаружения проникновения.

3.3.1 Классификация средств обнаружения проникновения.

Средства обнаружения проникновения (охранные извещатели), предназначенные для применения на объектах, классифицируют по следующим признакам функционального назначения.

3.3.1.1 По способу приведения в действие:

- автоматические;
- ручные (ножные).

3.3.1.2 По условиям эксплуатации:

- в отапливаемых помещениях;
- в помещениях с нерегулируемыми и неконтролируемыми параметрами температуры и влажности воздуха (в том числе под навесами);
- для эксплуатации на открытом воздухе.

3.3.1.3 По виду зоны, контролируемой автоматическим извещателем:

- точечные;
- линейные;
- поверхностные;
- объёмные.

3.3.1.4 По физическим принципам, положенным в основу обнаружения:

- электроконтактные;
- магнитоконтактные;
- ударноконтактные;
- емкостные;
- радиоволновые;

- оптико-электронные;
- вибрационные;
- звуковые (акустические).

3.3.1.5 По способу электропитания – на обеспечиваемые электропитанием от:

- источника постоянного тока;
- сети переменного тока;
- шлейфа сигнализации охранного приемно-контрольного прибора или оконечного объектового устройства системы передачи извещений;
- автономных источников.

3.3.1.6 По сочетанию принципов обнаружения:

- использующие один физический принцип;
- использующие два и более физических принципа: комбинированные, совмещенные.

3.3.2 Типы средств обнаружения, их назначение и функции.

Существует 12 типов средств обнаружения проникновений и угроз различных видов:

- магнитоконтактные извещатели для блокировки дверных, оконных конструкций и отдельных предметов;
- ударно-контактные извещатели для блокировки остеклённых конструкций;
- звуковые (акустические) извещатели для блокировки остеклённых конструкций;
- вибрационные извещатели для блокировки строительных конструкций и сейфов;
- ультразвуковые извещатели для блокировки объёма помещений;
- оптико-электронные пассивные извещатели для блокировки объёма помещений;
- оптико-электронные активные извещатели для блокировки проёмов помещений и отдельных предметов;
- радиоволновые извещатели для блокировки объёма помещений;
- ёмкостные извещатели для блокировки отдельных предметов;
- комбинированные извещатели для блокировки объёма помещений;
- совмещённые извещатели для блокировки объёма помещений и остеклённых конструкций;
- извещатели тревожной сигнализации (тревожные кнопки, педали).

3.3.2.1. Магнитоконтактные извещатели (Рисунок 1-4).

Магнитоконтактные извещатели применяют для блокировки «на открывание» подвижных строительных конструкций (дверей, окон, фрамуг, люков, ворот, т.п.), а также для блокировки «на перемещение» предметов (музейных или выставочных экспонатов, картин, товаров на витринах и стеллажах и т.п.).

Магнитоконтактные извещатели конструктивно состоят из двух частей: исполнительного блока (магнитоуправляемого датчика на основе геркона) и задающего блока, заключенного в отдельный корпус из «немагнитных» материалов (пластик, алюминий) управляющего элемента. В качестве управляющего элемента используют постоянный магнит, фрагмент магнитопровода или магнитопровод самой защитной конструкции.

Исполнительный блок извещателя устанавливают на неподвижную часть охраняемой конструкции, задающий блок – на перемещаемую (открываемую, сдвигаемую, наклоняемую) часть охраняемой конструкции.



Рисунок 1. Магнитоконтактный извещатель для блокировки дверных, оконных конструкций и отдельных предметов.



Рисунок 2. Магнитоконтактный извещатель для открытого монтажа на конструкциях, выполненных из магнитных материалов.



Рисунок 3. Магнитоконтактный извещатель для скрытого монтажа на конструкциях, выполненных из немагнитных материалов.



Рисунок 4. Магнитоконтактный извещатель для скрытого монтажа на конструкциях, выполненных из магнитных материалов.

Сигнал «тревога» данные извещатели выдают посредством размыкания контактов встроенного геркона.

В зависимости от конструктивного исполнения магнитоконтактные извещатели подразделяют на датчики, предназначенные для открытой установки на поверхности охраняемой конструкции и датчики для скрытой установки в охраняемую конструкцию.

3.3.2.2 Концевые выключатели.

Концевые выключатели конструктивно состоят из одного блока, применяются для блокировки ворот, люков на открывание (Рисунок 5).



Рисунок 5. Концевой выключатель.

3.3.2.3 Ударно-контактные извещатели (Рисунок 6).

Ударно-контактные извещатели предназначены для использования в составе систем охранной сигнализации с целью обнаружения разрушения установленного в строительной конструкции стекла или стеклопакета при попытке нарушителя проникнуть в защищаемое помещение через эту остекленную конструкцию.

Ударно-контактные извещатели состоят из блока обработки сигналов (БОС) и комплекта миниатюрных датчиков разрушения стекла, устанавливаемых непосредственно на стекла, охраняемые извещателем.

В ударно-контактных извещателях срабатывание геркона происходит под воздействием вибрационных колебаний определенной амплитуды, длительности и направления распространения, возникающих при разрушении стекла.

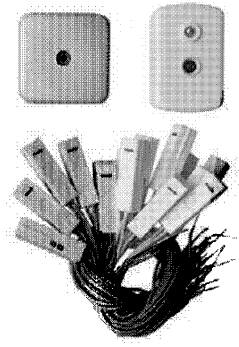


Рисунок 6. Ударно-контактные извещатели для остеклённых конструкций.

3.3.2.4 Извещатели охранные поверхностные звуковые (акустические) для блокировки остеклённых конструкций (Рисунок 7).

Извещатели охранные поверхностные звуковые (акустические) предназначены для обнаружения разрушения остеклённых конструкций в помещениях.

Дальность действия определяется расстоянием от извещателя до наиболее удалённой точки поверхности контролируемого стекла.

Минимальная охраняемая площадь представляет собой минимально допустимую для конкретного типа извещателя площадь поверхности охраняемого им стекла. Как правило, значение минимальной охраняемой площади устанавливают в диапазоне от 0,05 до 0,1 м^2.

Если в охраняемой конструкции установлены стёкла меньших размеров, то необходимо использовать извещатели другого принципа действия, например, ударно-контактные.



Рисунок 7. Извещатели охранные поверхностные звуковые (акустические) для блокировки остеклённых конструкций.

Не следует применять извещатели для блокировки стёкол, имеющих:

- толщину, не соответствующую диапазону, указанному в сопроводительной документации на извещатель;
- линейные размеры, не соответствующие требованиям к минимальной охраняемой площади, указанной в сопроводительной документации на извещатель;
- видимые повреждения (царапины, трещины, сколы и т.п.), снижающие прочность конструкции;
- некачественное (слабое, неплотное, ненадёжное) закрепление стекла в строительной конструкции (раме).

Для обеспечения надёжного обнаружения необходимо при установке извещателя ориентировать его зону обнаружения на блокируемые стёкла.

Для исключения ложных срабатываний от акустических помех извещатель не рекомендуется устанавливать в помещениях:

- с высоким уровнем звуковых шумов (более 65 дБ, что ориентировочно соответствует громкому разговору двух людей в помещении на удалении 3–4 м от извещателя);
- с плохой звукоизоляцией.

В помещении, на период его охраны, должны быть закрыты двери, форточки, отключены вентиляторы, радиоприёмники (или трансляционные громкоговорители) и другие возможные источники звуковых помех.

3.3.2.5 Вибрационные извещатели для блокировки строительных конструкций и сейфов (Рисунок 8).

Вибрационные извещатели предназначены для обнаружения на ранней стадии попытки умышленного разрушения, повреждения или взлома различных строительных конструкций (стены, перекрытия, двери и т.д.), металлических сейфов (шкафов).

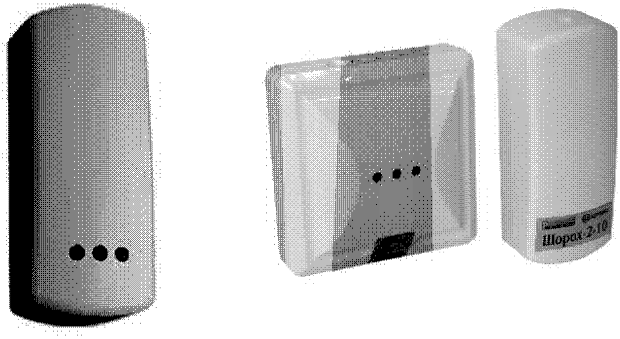


Рисунок 8. Вибрационные извещатели для блокировки строительных конструкций и сейфов (металлических шкафов).

Принцип действия вибрационных извещателей основан на анализе вибрационных сигналов, возникающих в строительных конструкциях при нанесении разрушающих воздействий с целью проникновения в охраняемое помещение.

С помощью таких извещателей можно защитить от вандализма лицевые панели банкоматов, организовать охрану конструкций, выполненных с применением многослойных защитных стёкол и стеклоблоков, кирпичных стен и перегородок, стальных решёток, деревянных дверей, оконных рам (при небольшом размере многосекционных остеклённых проёмов), перекрытий, конструкций из фанеры и древесностружечных плит.

Зона обнаружения вибрационного извещателя может охватывать смежные части сооружения, например, часть пола, потолка, примыкающей стены или капитальной перегородки, если угловое соединение жестко состыковано. В этих случаях дальность действия извещателя для смежных конструкций уменьшается приблизительно на 25 % от установленного значения (новое значение радиуса действия определяется опытным путём).

Охрана строительной конструкции может производиться посредством установки на ней одного или нескольких однопозиционных извещателей или нескольких датчиков вибрации многопозиционного извещателя.

Вибрационный многопозиционный извещатель состоит из блока обработки сигналов (БОС) и комплекта вибрационных извещателей, устанавливаемых непосредственно на охраняемую конструкцию.

Для охраны небольших конструкций, а также дверей, шкафов, сейфов или банкоматов, если их количество не превышает трёх, рекомендуется использовать однопозиционные извещатели, для охраны больших помещений или большого числа строительных конструкций – многопозиционные.

Извещатели обнаруживают разрушающие воздействия на охраняемые конструкции, производимые средствами взлома различной производительности и физического принципа действия, такими, как:

- ручные режущие инструменты (ручные дрели, пилы, напильники);
- термические режущие инструменты (газорежущее, электродуговое оборудование);
- электрические неударные инструменты (электродрели, дисковые пилы типа «болгарка»);
- электрические вращательные инструменты с ударом (электродрели с перфорацией, перфораторы);
- ручные ударные инструменты (молотки, кувалды, ломы, колуны, кирки);
- электрические ударные инструменты (отбойные молотки).

3.3.2.6 Ультразвуковые извещатели для блокировки объёма помещений (Рисунок 9, 10).

Ультразвуковой извещатель использует принцип активной локации.

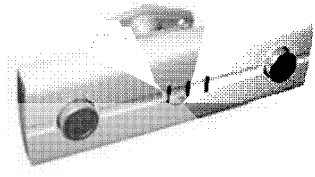


Рисунок 9. Ультразвуковой извещатель для блокировки объема помещения.

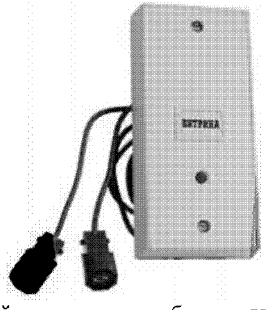


Рисунок 10. Ультразвуковой извещатель для блокировки внутреннего пространства витрин, экспозиций и небольших хранилищ ценностей.

Ультразвуковой извещатель для блокировки объема помещения предназначен для обнаружения движения нарушителя или выявления открытого очага пламени в охраняемой зоне.

При выборе данного извещателя для охраны того или иного объекта необходимо иметь в виду, что акустические волны ультразвукового диапазона, создаваемые извещателем, обладают способностью отражаться от любых твёрдых поверхностей, а также огибать препятствия сравнительно небольших размеров.

Поэтому есть возможность минимизировать образование так называемых «мёртвых зон» (зон нечувствительности).

На функционирование извещателя практически не влияют звуковые помехи, возникающие снаружи охраняемого помещения.

Перемещение мелких домашних животных (грызунов) в зоне обнаружения не вызывает ложных срабатываний извещателя, так как отражающая поверхность этих «нарушителей» (с учётом их малых размеров и наличия шерсти, поглощающей ультразвук) является пренебрежительно малой для извещателя.

Ультразвуковой извещатель для блокировки внутреннего пространства витрин, экспозиций и небольших хранилищ ценностей предназначен для обнаружения проникновения (попытки проникновения) в охраняемую витрину (объём), перемещения предметов в охраняемом объёме.

Извещатель обеспечивает контроль всего объёма охраняемой конструкции путем создания стационарного акустического поля.

3.3.2.7 Оптико-электронные пассивные инфракрасные (ИК) извещатели для блокировки объёма помещений и проёмов в строительных конструкциях (Рисунок 11).

Оптико-электронные пассивные ИК извещатели разделяются по типу формируемой зоны обнаружения (ЗО):

- объёмные;
- поверхностные;
- линейные.



Рисунок 11. Извещатели оптико-электронные пассивные ИК.

Они предназначены для обнаружения нарушителя, перемещающегося или пересекающего ЗО.

Извещатели, формирующие объёмную ЗО, в свою очередь, подразделяются по способу установки (на стене или на потолке).

Пассивные оптико-электронные ИК извещатели имеют одноблочную конструкцию.

Принцип действия пассивных оптико-электронных ИК извещателей основан на регистрации изменения уровня теплового излучения.

Извещатель рекомендуется устанавливать таким образом, чтобы в его ЗО не попадали потоки тёплого воздуха. В период охраны в помещении должны быть закрыты окна (форточки, фрамуги), балконные и входные двери, отключены обогревательные вентиляторы, кондиционеры и т.п.

Если температура окружающего воздуха ниже (при установке в неотапливаемых помещениях) или выше допустимых значений рабочей температуры извещателя, то извещатель может не обнаруживать нарушителя.

Наличие на входном окне извещателя постоянной или переменной высокой освещённости, фактическое значение которой превышает 6500 лк (ГОСТ Р 50777-14 «Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний»), может являться причиной ложных срабатываний или пропуска нарушителя.

Причиной высокой освещённости может быть как солнце, так и источники искусственного освещения.

Для исключения влияния данного фактора на работу извещателя он должен быть установлен таким образом, чтобы на его входное окно не попадали прямые солнечные лучи и излучение от мощных осветительных приборов.

Следует иметь в виду, что резкое чередование на входном окне извещателя света и тени (вызванное, к примеру, перемещающимися по небу облаками, качающимися ветвями деревьев, перекрывающими солнце и т.п.) негативно влияет на работу извещателя и может являться причиной ложных срабатываний. При этом следует отметить, что сами качающиеся за окном ветки влияния на работоспособность пассивного ИК извещателя, установленного в помещении (при условии, что окна помещения закрыты, что обычно оговаривается в прилагаемой к извещателю эксплуатационной документации), не оказывают.

Оседание на входном окне извещателя твердых мелкодисперсных частиц приводит к уменьшению максимальной рабочей дальности действия и обнаружительной способности извещателя.

При наличие в ЗО крупногабаритных предметов и конструкций (сплошные, сетчатые, стеклянные перегородки), перемещение нарушителя за ними обнаружено не будет.

При этом обеспечить полное отсутствие таких предметов на большинстве объектов невозможно. В этом случае для обеспечения

надёжной охраны необходимо установить несколько извещателей таким образом, чтобы все возможные пути перемещения нарушителя попадали в их ЗО.

Наличие на охраняемом объекте животных, перемещающихся в ЗО извещателя, может привести к ложному извещению о тревоге.

Для охраны таких объектов необходимо применять специальные извещатели, обладающие устойчивостью к перемещению в ЗО животных, а при выборе места их установки и монтаже строго выполнять требования, изложенные в прилагаемой к извещателям эксплуатационной документации.

3.3.2.8 Оптико-электронные активные ИК извещатели для блокировки периметров, конструкций, помещений и отдельных предметов (Рисунок 12, 13).

Линейные оптико-электронные извещатели (активные ИК извещатели) предназначены для обнаружения попыток проникновения на охраняемый объект и формирования извещения о тревоге. В отличие от пассивных ИК извещателей, регистрирующих тепловое излучение нарушителя, активные ИК извещатели регистрируют изменение собственного излучения, вызванное вторжением нарушителя в ЗО.

Достоинством активных ИК извещателей является то, что их обнаружительная способность не зависит от характеристик теплового излучения человека (нарушителя). Также они нечувствительны к изменению характеристик теплового излучения окружающих объектов (фона) и возникающим тепловым помехам.

К недостаткам активных ИК извещателей можно отнести то, что они способны формировать только линейную ЗО, что ограничивает их область применения. Отчасти эта проблема может быть решена путём организации поверхностной ЗО (так называемого ИК барьера) за счёт применения извещателей, формирующих несколько ИК лучей, или построения ИК барьера из нескольких извещателей. Но при этом размеры ЗО для первого варианта будут небольшими, а второй вариант потребует увеличения финансовых затрат. К недостаткам можно отнести и их чувствительность к оптическим засветкам.

Активные ИК извещатели, как правило, имеют двухблочную конструкцию (Рисунок 12) и состоят из блока излучателя (БИ) и блока фотоприёмника (БФ), образующих оптическую систему.

Появление в ЗО извещателя оптически непрозрачного объекта вызывает прерывание (или снижение мощности) ИК луча, попадающего в приёмник, который анализирует величину и длительность этого прерывания в соответствии с заданным алгоритмом, формирует извещение о тревоге путём изменения сопротивления контактов, подключаемых к шлейфу сигнализации.



Рисунок 12. Активные линейные двухблочные ИК извещатели.

Извещатели, имеющие одноблочную конструкцию (Рисунок 13), состоят из излучателя и фотоприёмника, объединённых в одном корпусе, и светоотражателя (катафота).

Активными ИК извещателями удобно блокировать проёмы ворот, имеющихся в здании (например, ворота боксов или гаражей для хранения автотранспорта). Помимо прохода человека через проём, извещатель будет обнаруживать и проезд транспортного средства. Если ворота имеют распашную конструкцию и их створки открываются наружу, извещатель также будет обнаруживать факт открытия ворот.



Рисунок 13. Активный линейный одноблочный (с катафотом) ИК извещатель.

Блокировка окон, световых фонарей ИК извещателями установленными снаружи здания, применяется для обнаружения проникновения в здание через проём, и для обнаружения попыток несанкционированного воздействия на оконные конструкции (нередки случаи попыток проникновения в здание через оконный проём путём вынимания стекла без его разрушения, при котором акустические извещатели, установленные в здании, извещение о тревоге не формируют).

3.3.2.9 Радиоволновые извещатели для блокировки объема помещений (Рисунок 14).



Рисунок 14. Радиоволновые извещатели для блокировки объема помещений.

В основе принципа действия радиоволновых извещателей лежит эффект Доплера. При отражении сверхвысокочастотного (СВЧ) радиосигнала от движущегося объекта его частота изменяется.

По конструкции извещатели, как правило, имеют одноблочную схему, в которой содержатся два основных узла: СВЧ модуль, который излучает и принимает сверхвысокочастотные колебания, и процессор, который по определённому алгоритму анализирует параметры доплеровского сигнала, поступающего со смесителя, и принимает решение о формировании извещения о тревоге.

При работе извещателя создаётся объёмная зона обнаружения. Электромагнитное излучение распространяется в объёме помещения и ограничивается его капитальными конструкциями.

Вместе с тем, излучение может проникать в соседнее помещение через перегородки, изготовленные на основе древесностружечных плит, фанеры, гипсокартона и т.д., через деревянные и пластмассовые двери, на улицу – через оконные проёмы. В этом случае движение людей, крупных животных, автомобилей за габаритами помещения может привести к формированию ложной тревоги.

Радиоволновые извещатели, предназначенные для блокировки объёма помещений, сохраняют работоспособность в широком диапазоне температур, не реагируют на световые засветки, тепловые потоки и сквозняки, имеют стабильную объёмную зону обнаружения, допускают маскировку радиопрозрачными материалами.

Извещатели могут формировать ложные тревоги от вибрации крупных предметов, люминесцентного освещения, перемещения людей или механизмов за оконными проёмами или тонкими перегородками.

3.3.2.10 Комбинированные извещатели для блокировки объема помещений (Рисунок 15, 16).



Рисунок 15. Комбинированный (СВЧ + ИК) извещатель для блокировки объема помещения (устанавливается на стене).



Рисунок 16. Комбинированный (СВЧ + ИК) извещатель для блокировки объема помещения (устанавливается на потолке).

Рекомендуемая область применения комбинированных (СВЧ + ИК) извещателей – блокировка объёма помещений с повышенным уровнем помех, мест сосредоточения ценностей, музейных экспонатов, оргтехники, а также помещений критически важных объектов.

В извещателях этого класса используются два физических принципа обнаружения движущегося объекта: регистрация изменения теплового фона, возникающего при пересечении чувствительных зон, формируемых оптической системой, и регистрация наличия доплеровской составляющей в спектре отражённого сигнала, создаваемого СВЧ модулем. При появлении нарушителя в зоне обнаружения срабатывают оба канала (в любой

последовательности, с разнесением по времени), формируется извещение о тревоге.

Комбинированные извещатели обладают повышенной помехоустойчивостью по сравнению с собственно радиоволновыми или пассивными ИК извещателями, так как вероятность возникновения в помещении помех, одновременно воздействующих на два канала, достаточна мала.

Комбинированные (СВЧ + ИК) извещатели надёжно работают в помещениях с повышенным уровнем помех, в которых радиоволновые или оптико-электронные пассивные извещатели, функционирующие по отдельности, выдают ложные извещения о тревоге.

3.3.2.11 Комбинированные (ультразвуковые + ИК) извещатели для блокировки объёма помещений (Рисунок 17).

Основная область применения комбинированных (ультразвуковых + ИК) извещателей – помещения, имеющие следующие особенности:

- со сложной помеховой обстановкой внутри и снаружи помещения;
- с остеклёнными (оконными, дверными) конструкциями, выходящими на оживлённую улицу, в том числе остеклённые вестибюли зданий, бизнес-центров, магазинов, выставочных павильонов;
- имеющие некапитальные стены или перегородки со смежными помещениями, где возможно нахождение людей в период охраны.

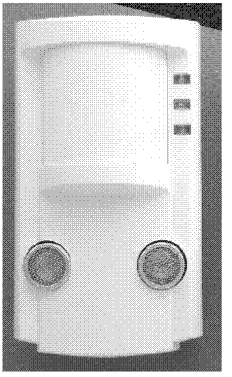


Рисунок 17. Комбинированный (ультразвуковой + ИК) извещатель для блокировки объема помещений.

Принцип работы комбинированных (ультразвуковых + ИК) извещателей заключается в комбинировании двух принципов обнаружения стандартной цели (человека) в охраняемом помещении.

Первый принцип заключается в регистрации ИК излучения при пересечении человеком элементарных зон обнаружения, формируемых оптической системой ИК канала извещателя.

Второй принцип работы извещателя основан на эффекте Доплера, в соответствии с которым частота ультразвукового сигнала, отражённого от движущегося препятствия, отличается от первоначальной на величину, которая прямо пропорциональна излучаемой частоте и радиальной скорости движения отражателя и обратно пропорциональна скорости распространения ультразвука в контролируемой среде.

Следует отметить, что размеры зоны можно изменять так, как требуется в конкретных условиях (габаритах помещения), в том числе для создания локального охраняемого пространства.

3.3.2.12 Совмещённые извещатели для блокировки объёма помещений и остеклённых конструкций (Рисунок 18).

Область применения совмещённых (ИК + акустический) извещателей – помещения с остеклёнными (оконными, дверными) конструкциями.



Рисунок 18. Совмещённые извещатели для блокировки объема помещений и остеклённых конструкций.

Извещатели сочетают в себе два принципа обнаружения (ИК + акустический), обнаруживают движение нарушителя в закрытом охраняемом помещении и разрушение строительных конструкций, выполненных с использованием листового стекла (обычного, армированного, узорчатого, закалённого, трёхслойного, ударостойкого), стеклоблоков, однокамерных и двухкамерных стеклопакетов.

При появлении человека в зоне обнаружения срабатывает ИК канал обнаружения, при разбитии стекла – акустический канал (в любой последовательности или одновременно). При этом выдаётся извещение о тревоге путем размыкания контактов соответствующего выходного реле.

3.3.2.13 Извещатели для тревожной сигнализации (ТС) о нападении (тревожные кнопки, педали и т.п.).

Для оперативной передачи сообщений в дежурную часть органов внутренних дел или на ПЦН о нападении нарушителя объект оборудуют техническими средствами ТС.

Извещатель (Рисунок 19) представляет собой тревожную кнопку для выдачи извещения о нападении с фиксацией извещения. Перевод извещателя в дежурный режим после нажатия кнопки осуществляется при помощи ключа, который хранится в подразделении охраны.



Рисунок 19. Тревожная кнопка с фиксацией.

Извещатель (Рисунок 20) предназначен для подачи сигнала тревоги ногой при нападении преступников на сотрудников.

Система ТС должна быть выполнена «без права отключения», выведена на пульт внутренней охраны, на ПЦН.



Рисунок 20. Тревожный извещатель для подачи сигнала тревоги ногой при нападении преступников.

3.4 Критерии выбора СОТС.

Критерии выбора СОТС:

- назначение и функции, выполняемые техническими средствами охранной сигнализации;
- вид предполагаемой угрозы объекту;
- помехозащищённость;
- надёжность;
- круглосуточный режим функционирования;
- функционирование в автоматическом режиме;
- функционирование в автономном режиме;
- самодиагностирование;
- бесперебойное электропитание;
- возможность расширения как функциональных, так и количественных характеристик системы;
- интеграция в единую систему безопасности;
- защита информации от несанкционированного внешнего доступа и копирования при передаче от периферийных узлов на пульт дежурного;

– соответствие российским и международным стандартам.

3.5 Организация передачи информации на пульт централизованного наблюдения.

3.5.1 Передача извещений о срабатывании охранной сигнализации (ОС) с объекта на ПЦН может осуществляться с ППК, внутреннего пульта охраны или УОО СПИ.

3.5.2 Количество рубежей ОС, выводимых на ПЦН отдельными условными номерами, определяется совместным решением руководителя объекта и подразделения вневедомственной охраны исходя из категории объекта, анализа риска и потенциальных угроз объекту, возможностей интеграции и документирования ППК (внутренним пультом охраны или УОО СПИ) поступающей информации, а также порядком организации дежурства на объекте.

3.5.3 При наличии на объекте пульта внутренней охраны с круглосуточным дежурством на ПЦН выводятся:

– один общий сигнал, объединяющий все рубежи ОС объекта, за исключением рубежей специальных помещений объекта;
– рубежи ОС (периметр и объём) специальных помещений.

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

3.5.4 При наличии на объекте пульта внутренней охраны с круглосуточным дежурством сотрудников подразделений вневедомственной охраны (Микро–ПЦН), все рубежи ОС помещений объекта (включая и специальные помещения) подключаются на пульт внутренней охраны, обеспечивающий автоматическую регистрацию всей поступающей информации, а с него выводится один общий сигнал на ПЦН.

На объектах, где охраняются только специальные помещения, выводу на ПЦН подлежат все рубежи ОС этих помещений.

3.5.5 Рубежи ОС должны выводиться на ПЦН с пульта внутренней охраны, ППК или УОО СПИ, обеспечивающих запоминание тревожного состояния и его фиксацию на выносном световом (звуковом) оповещателе или индикаторе.

Извещения от шлейфов ОС одним объединенным сигналом выводятся на ПЦН и в дежурную часть органов внутренних дел Российской Федерации непосредственно или через ППК, УОО СПИ, пульт внутренней охраны.

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

3.5.7 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 ПЦН в составе ТС.

3.5.8 Извещения СОТС могут передаваться на ПЦН 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 с обязательным контролем канала между охраняемым объектом и ПЦН.

Проводная среда передачи информации реализуется в виде:

- абонентской телефонной сети общего пользования или специально прокладываемой выделенной линии оператора связи (технология DSL, FTTC, FTTB, в т.ч. по технологии GPON);
- линии связи интернет провайдеров (коаксиальный кабель, «витая пара», оптоволоконный кабель);

Беспроводная среда передачи информации может быть реализована в виде:

- выделенных рабочих частот УКВ радиодиапазона;
- защищённых каналов передачи данных сетей сотовых операторов стандарта GSM(GPRS) - VPN.

3.6 Электропитание.

СОТС, согласно Р 78.36.032-2013 (п. 9) и ПУЭ (п. 1.2.17.), относится к 1 категории электроприёмников по надёжности электроснабжения, в силу чего электропитание должно быть бесперебойным.

При пропадании основного электропитания 220 В, 50 Гц СОТС автоматически переходит на электропитание от резервного источника электропитания (аккумулятора) постоянного напряжения 12 В без выдачи сигналов тревоги, но с формированием служебного сообщения «переход на резервное электропитание».

При переходе на электропитание от резервного источника электропитания (аккумулятора) должна обеспечиваться бесперебойная работа оборудования и извещателей СОТС не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги.

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

- в городах и поселках городского типа – до 4 часов в дежурном режиме и до 1 часа в режиме тревоги;
- 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.

Пример расчёта резервного источника электропитания при наличии автоматического или иного оповещения подразделения вневедомственной охраны о моменте отключения основного электропитания в городах и поселках городского типа - до 4 часов в дежурном режиме и до 1 часа в режиме тревоги.

№	Наименование	Кол-во, шт.	Ток потребления одним устройством в дежурном режиме, мА	Ток потребления одним устройством в режиме тревоги, мА	Суммарный ток потребления в дежурном режиме, мА	Суммарный ток потребления, в режиме тревоги, мА
1	Пульт контроля и управления охранно-пожарный	1	60	120	60	120
2	Прибор приёмно-контрольный ёмкостью на 20 шлейфов	2	600	650	1200	1300
3	Релейный модуль	1	300	300	300	300
4	Пульт непрограммируемый	1	60	120	60	120
5	Устройство оконечное объектовое СПИ	1	150	250	150	250
6	Извещатель охранный объёмный радиоволновый	4	25	25	100	100
7	Извещатель охранный объёмный оптико-электронный	10	20	20	200	200
8	Извещатель охранный поверхностный оптико-электронный	8	20	20	160	160
9	Извещатель охранный поверхностный звуковой	10	20	20	200	200
10	Радиоприёмник	1	80	80	80	80
	ИТОГО				2510	2830

Необходимая ёмкость аккумулятора рассчитывается по формуле:
Q(мАч) = 1,2 x Iр(мА) x t(ч),
где:
1,2 - коэффициент запаса ёмкости;

Ip - потребляемый ток (мА);

t - требуемое время работы (ч).

Необходимая ёмкость аккумулятора в дежурном режиме составляет:

1,2 х 2510 мА х 4 ч =12488 мАч.

Необходимая ёмкость аккумулятора в режиме тревоги составляет:

1,2 х 2830 мА х 1 ч = 3396 мАч.

12488 мАч.+ 3396 мАч.=15884 мАч.

Согласно расчётам выбираем резервированный источник электропитания, удовлетворяющий следующим характеристикам:

– максимальный ток нагрузки не менее 2,83 А;

– ёмкость аккумулятора должна быть не менее 15,884 Ач.

Заземление оборудования и устройств должно выполняться в соответствии с требованиями СНиП 3.05.06-85, ПУЭ, технической документации предприятий-изготовителей.

3.7 Общие требования к минимально необходимому составу СОТС.

3.7.1 Требования к защите СОТС зданий, помещений, отдельных предметов.

ТСО должны оборудоваться все помещения с постоянным или временным хранением материальных ценностей, а также все уязвимые места здания (окна, двери, люки, вентиляционные шахты, короба и другие проемы), через которые возможно несанкционированное проникновение в помещения объекта.

Для защиты вентиляционных шахт, коробов и дымоходов сечением более 200 мм, имеющих выход за границы охраняемой территории объекта, в том числе на крыши зданий, а также в смежные неохраняемые помещения и своим сечением входящие в охраняемые помещения, допускается использование фальшрешёток с ячейкой 100 х 100 мм, выполненных из металлических трубок с диаметром отверстия не менее 6 мм для протяжки провода шлейфа сигнализации «на обрыв», а также применение иных ТСО.

В случае наличия на охраняемых объектах неиспользуемых подвальных помещений необходимо, при отсутствии двери на выходе из них, установить металлическую открывающуюся решётчатую дверь, закрывающуюся на навесной замок, и оснастить её ТСО.

Ключи от замков на оконных решётках и дверях запасных выходов должны быть размещены в непосредственной близости или в специально выделенном помещении (в помещении охраны) в ящике, шкафу или нише, заблокированных ОС.

Устанавливаемые ТСО СОТС должны вписываться в интерьер помещения и по возможности устанавливаться скрытно.

В разных рубежах ОС необходимо применять охранные извещатели, работающие на различных физических принципах действия.

Количество шлейфов ОС должно определяться тактикой охраны, размерами зданий, строений, сооружений, этажностью, количеством

уязвимых мест, а также точностью определения места проникновения для быстрого реагирования на извещения о тревоге.

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

Для усиления охраны и повышения её надежности на объектах следует устанавливать дополнительные извещатели-ловушки. Сигналы ловушек выводятся по самостоятельным или, при отсутствии технической возможности, по имеющимся шлейфам ОС.

В помещениях, где круглосуточно должны находиться сотрудники полиции, ОС должны оборудоваться отдельные участки периметра помещения, а также сейфы и металлические шкафы для хранения ценностей и документов.

Помещения объектов оборудуются многорубежной системой ОС, а вспомогательные помещения – однорубежной.

3.7.2 Охранная сигнализация.

ОС оборудуются:

- периметр зданий (помещений) и сооружений (оконные проемы, двери, люки, ворота и другие) с выводом на внутренний пост охраны (дежурная часть) и ПЦН;
- отдельные служебные помещения с выводом на внутренний пост охраны (дежурную часть) и ПЦН;
- специальные помещения с выводом на внутренний пост охраны (дежурную часть) и ПЦН.

Первым рубежом ОС, в зависимости от вида предполагаемых угроз объекту, блокируют:

- входные двери, погрузочно-разгрузочные люки, ворота – на «открывание», «разрушение» и «пролом»;
- деревянные, стеклянные и остеклённые конструкции – на «открывание», «разрушение» и «разбитие» стекла;
- стены, перекрытия и перегородки, за которыми размещаются помещения других собственников – на «разрушение» и «пролом»;
- вентиляционные короба, дымоходы, места ввода/вывода коммуникаций сечением более 200 х 200 мм – на «разрушение» и «пролом».

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

Вторым рубежом ОС защищаются объемы помещений на «проникновение» с помощью объёмных извещателей различного принципа действия.

Третьим рубежом ОС в помещениях блокируются отдельные предметы, сейфы, металлические шкафы, в которых сосредоточены документы и ценности.

Специальные помещения.

Специальные помещения: для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, архивы, хранилища, кассы и другие защищаются в два рубежа охраны.

Первым рубежом ОС блокируются:

1. Входные двери в помещения – на открывание;
2. Окна – на открывание и разбитие.

Вторым рубежом ОС – объём помещения.

Дополнительным рубежом ОС в помещениях могут блокироваться отдельные предметы, сейфы, металлические шкафы, в которых сосредоточены документы и ценности.

Для блокировки помещений двумя (тремя) рубежами охраны применяются охранные извещатели, работающие на различных физических принципах действия.

3.7.3 Тревожная сигнализация.

Для передачи тревожных извещений в дежурную часть о противоправных действиях в отношении сотрудников и работников (угроз террористического и криминального характера) объект оборудуется устройствами ТС.

Устройства тревожной сигнализации на объекте должны устанавливаться:

- в специальных помещениях (дежурных частей, комнатах хранения оружия, боеприпасов и специальных средств, для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, архивах, хранилищах, кассах и других);
- у центрального входа в здание и запасных выходов из него;
- на всех наружных и внутренних постах охраны и в помещении охраны;
- в иных местах, регламентированных правовыми актами МВД России.

Рекомендуется использовать мобильные устройства ТС, работающие по радиоканалу (радиокнопки или радиобрелоки).

Устройства тревожной сигнализации размещаются в местах, по возможности незаметных для посетителей.

Решение о необходимости вывода сигнала на ПЦН принимается руководителем подразделения, в ведении которого находится объект, исходя из его функционального назначения, степени потенциальной опасности,

которой он может подвергаться, а также анализа вероятных угроз объекту и характеристики его уязвимости.

Обобщённый сигнал от КТС подключается на ПЦН без права отключения.

Примечания:

1. Аттестованные помещения, а также помещения, предназначенные для обработки сведений, составляющих государственную тайну, оборудуются техническими средствами ОС, прошедшими сертификацию по стандартам ФСТЭК России и ФСБ России.

2. В случае отсутствия (с учетом объективных факторов) на объекте необходимых средств инженерно-технической укреплённости (решётки на окнах и т.д.) либо оснащённости объекта средствами инженерно-технической укреплённости более низкого класса защиты, рекомендуется оборудовать объект дополнительными рубежами охраны с использованием средств охранной сигнализации и системы охранной телевизионной.

Организация дополнительных рубежей охраны должна быть согласована с подразделением охраны и руководством объекта.

ПРИЛОЖЕНИЯ

Приложение 1

Условные обозначения

Наименование	Обозначение
Пульт управления программируемый	
Прибор приемно-контрольный охранно-пожарный	
Устройство взятия-снятия СПИ	
Устройство оконечное объектовое СПИ	
Релейный блок	
Извещатель охранный магнитоконтактный для деревянных окон, дверей	
Извещатель охранный магнитоконтактный для металлических дверей	
Извещатель охранный поверхностный оптико-электронный (пассивный ИК)	
Извещатель охранный объемный оптико-электронный (пассивный ИК)	
Извещатель охранный объемный радиоволновый	
Извещатель охранный поверхностный вибрационный	
Извещатель охранный совмещенный вибрационный с датчиком наклона.	
Извещатель охранный поверхностный звуковой (акустический)	
Извещатель охранный омический	
Кнопка тревожной сигнализации	
Оповещатель охранно-пожарный световой	
Оповещатель охранно-пожарный звуковой	
Источник резервированного электропитания 12В	
Бесперебойный источник питания 220В	
Адресная линия связи	
Шлейф сигнализации	

Приложение 2

Схема блокировки двери, окна извещателем охранным магнитоконтактным

Схема блокировки двери

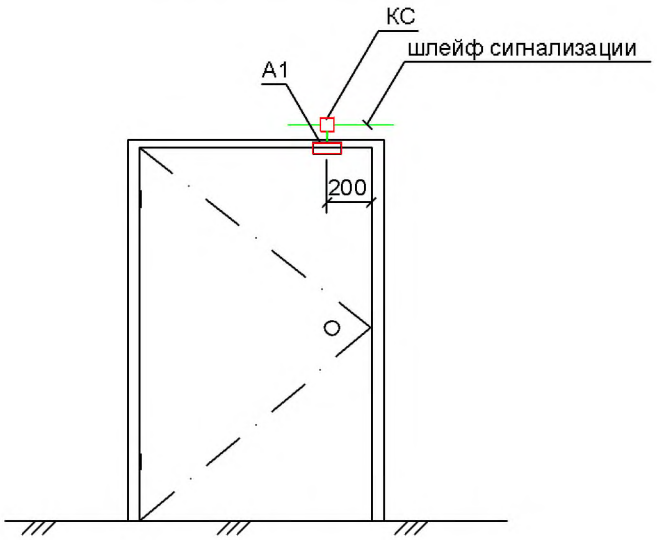
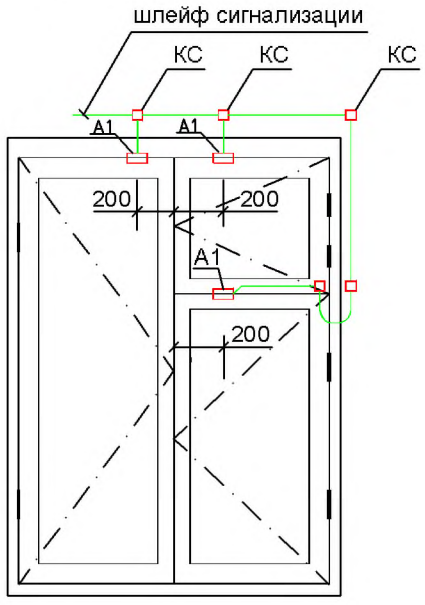


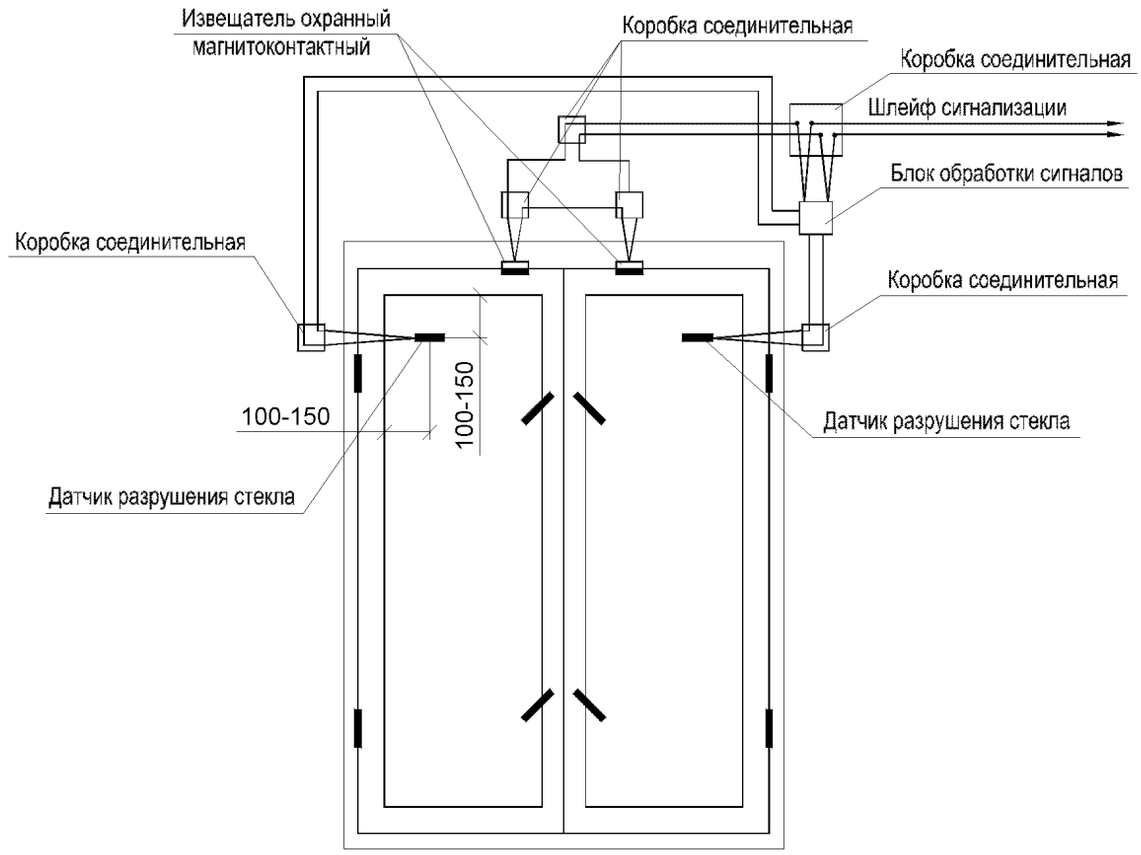
Схема блокировки окна



А1- Извещатель охранный магнитоконтактный
КС- Коробка соединительная

Приложение 3

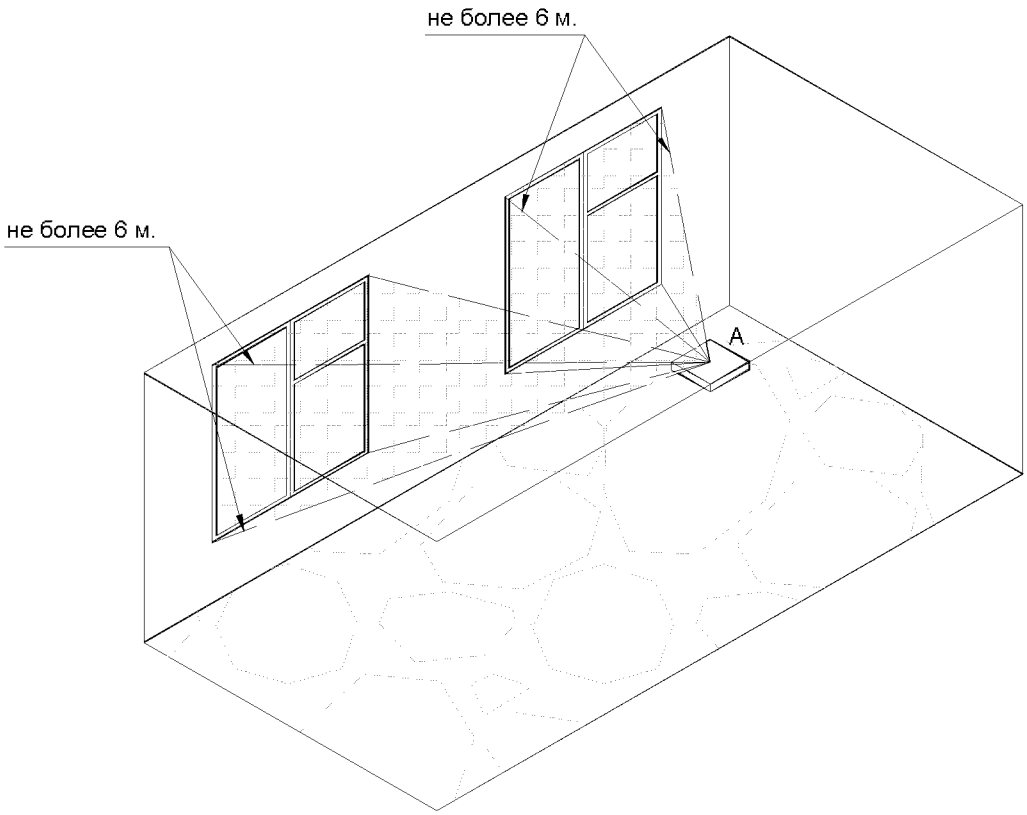
Схема установки извещателя охранного ударно-контактного для блокировки окна



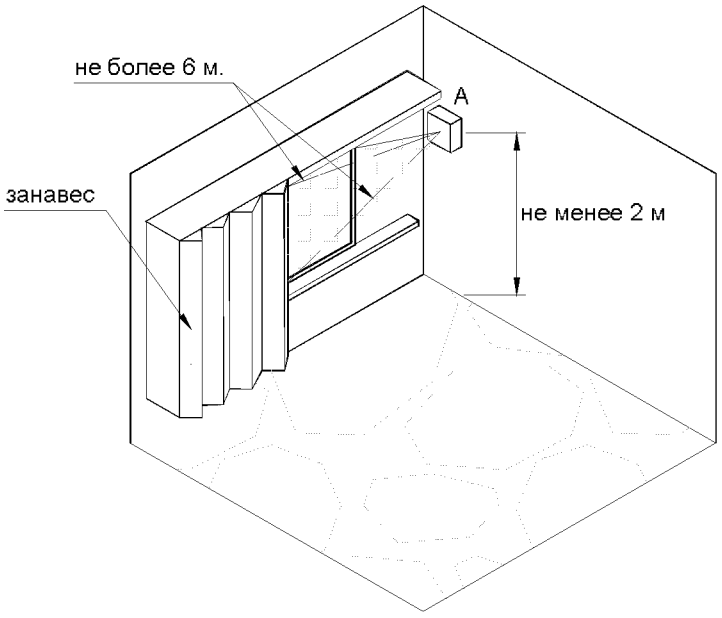
Приложение 4

Схема установки извещателя охранного поверхностного звукового (акустического)

Установка на потолке



Установка извещателя между стеклом и занавесом (жалюзи)



А-Извещатель охранный поверхностной звуковой (акустический)

Приложение 5

Схема установки извещателя охранного поверхностного оптико-электронного (инфракрасного)

Зоны обнаружения

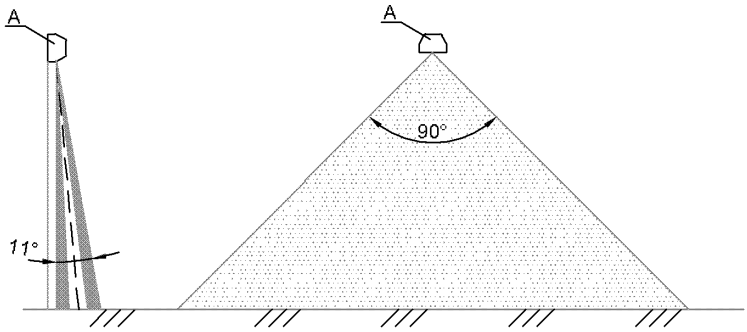
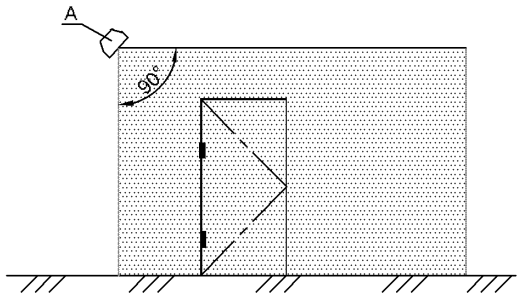


Схема блокировки двери



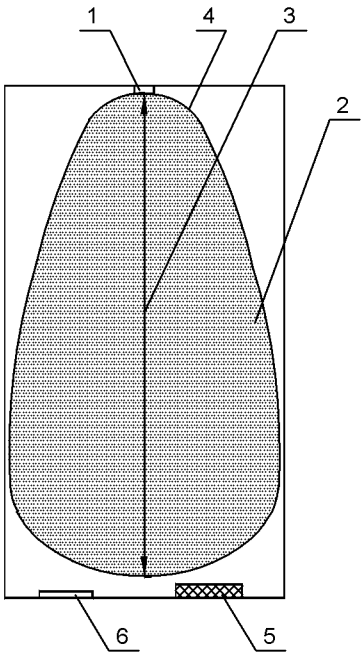
А-Извещатель охранный поверхностной оптико-электронный

Приложение 6

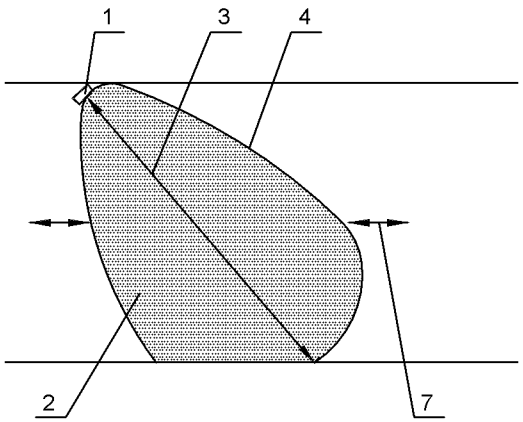
Схема установки извещателя охранного объемного ультразвукового

Вид сверху

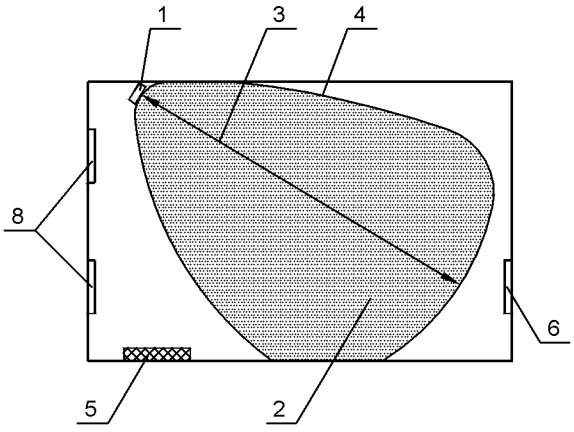
Вариант 1



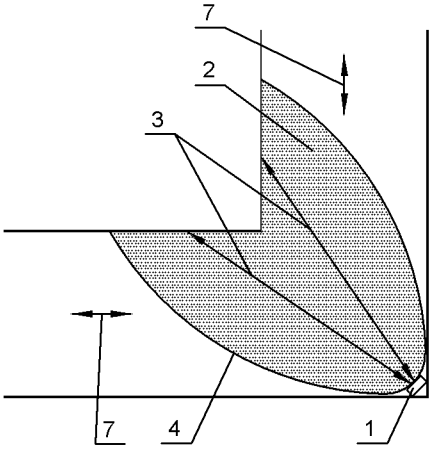
Вариант 2



Вариант 3



Вариант 4

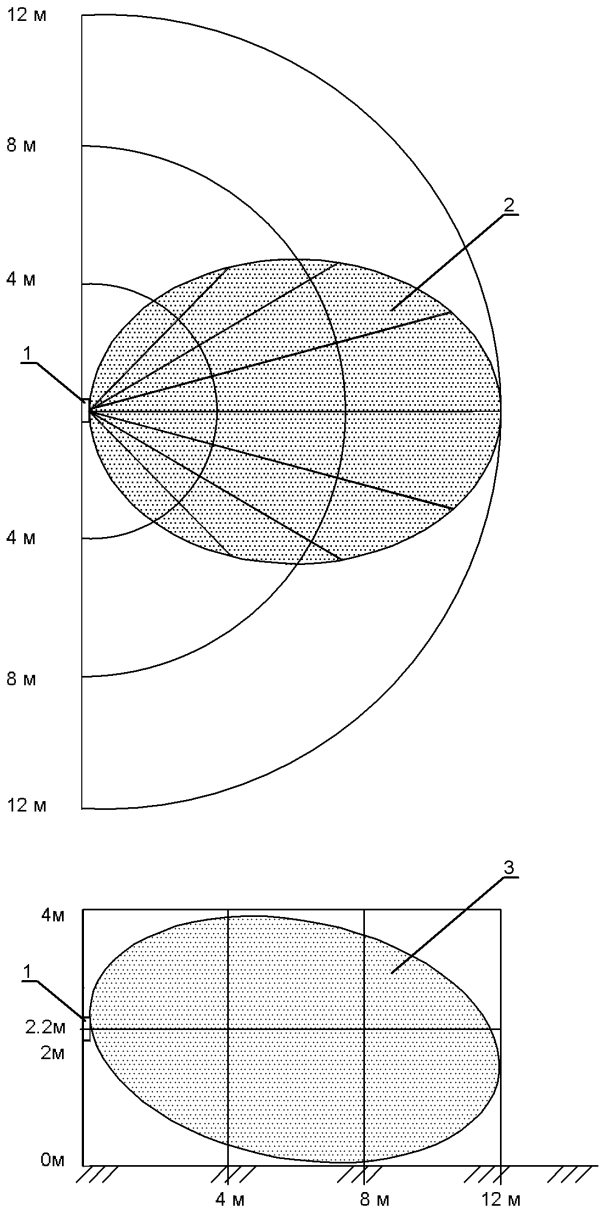


1-извещатель
2-зона обнаружения (ЗО)
3-дальность действия (осевая линия ЗО)
4-граница ЗО
5-электрообогреватель или батарея отопления
6-дверь
7-наиболее вероятное направление движения нарушителя
8-окно

Приложение 7

Схема установки извещателя охранного объемного радиоволнового

Зоны обнаружения



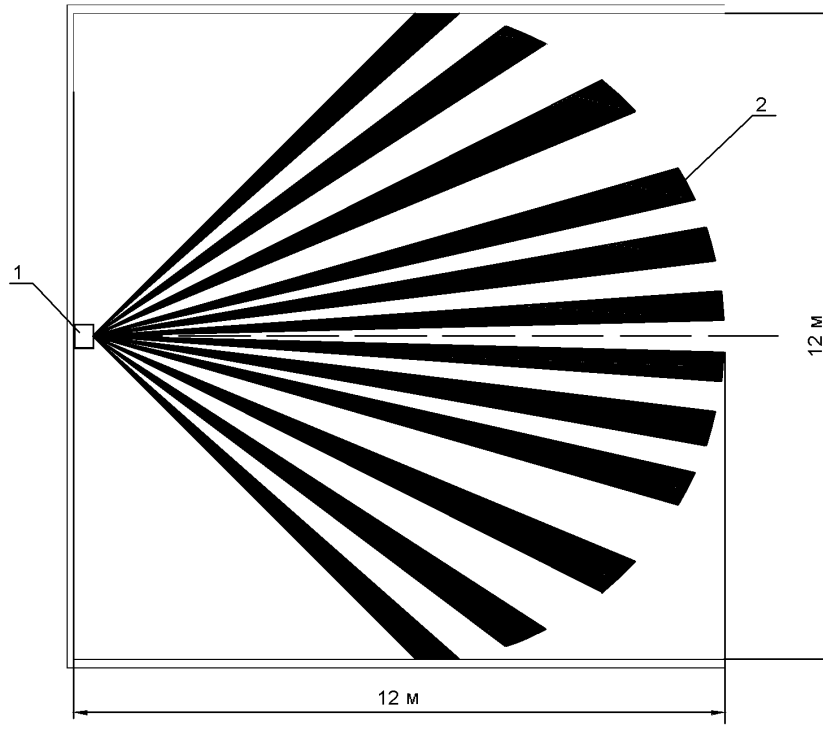
1-Извещатель охранный объемный радиоволновой
2-Зона обнаружения в горизонтальной плоскости
3-Зона обнаружения в вертикальной плоскости

Приложение 8

Схема установки извещателя охранного объемного оптико-электронного (инфракрасного)

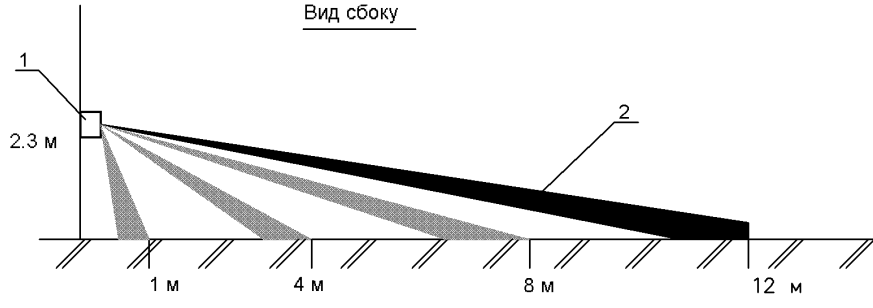
Оптико-электронный канал

Вид сверху



Оптико-электронный канал

Вид сбоку

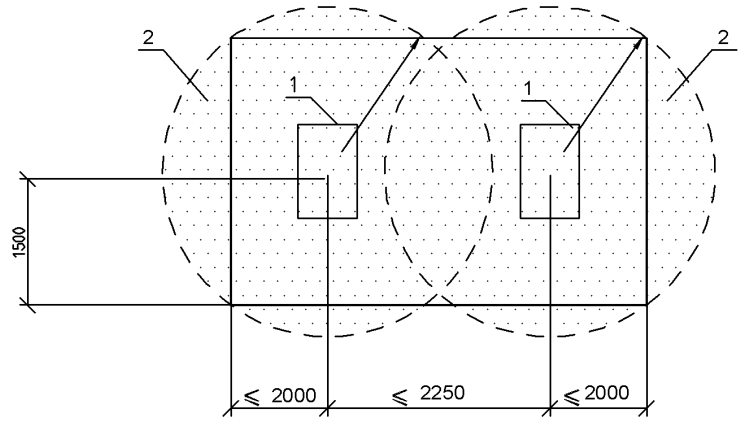


1-Извещатель охранный оптико-электронный (инфракрасный)
2-Зона обнаружения

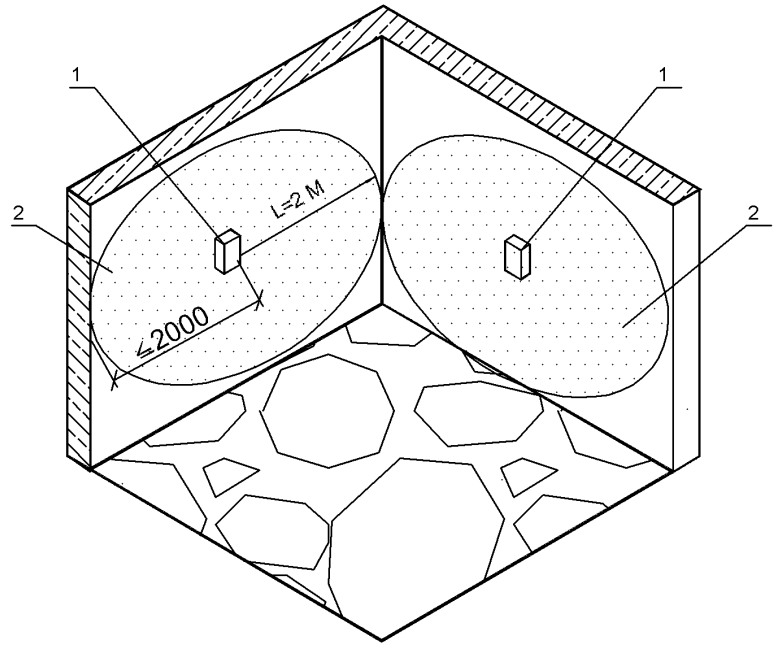
Приложение 9

Схема установки извещателя охранного поверхностного вибрационного на стене

Зоны обнаружения



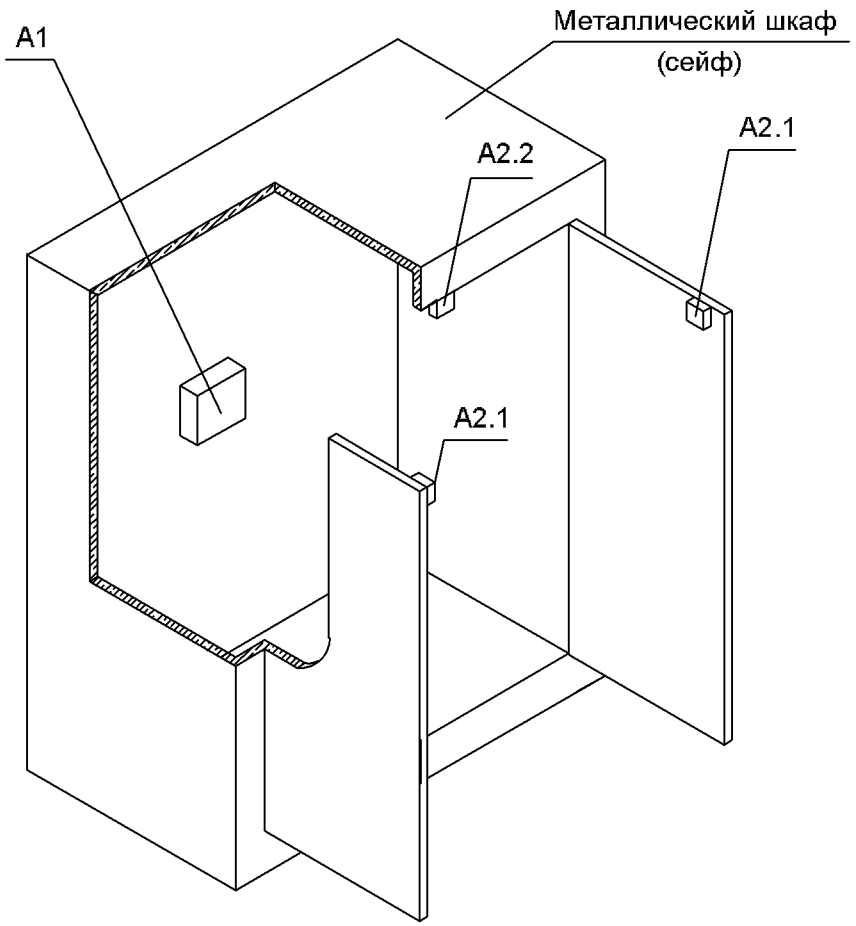
Полная защита конструкции



1- Извещатель охранный поверхностный вибрационный.
2- Зона обнаружения

Приложение 10

Схема установки извещателя охранного поверхностного вибрационного с датчиком наклона



A1- Извещатель охранный поверхностный вибрационный с датчиком наклона

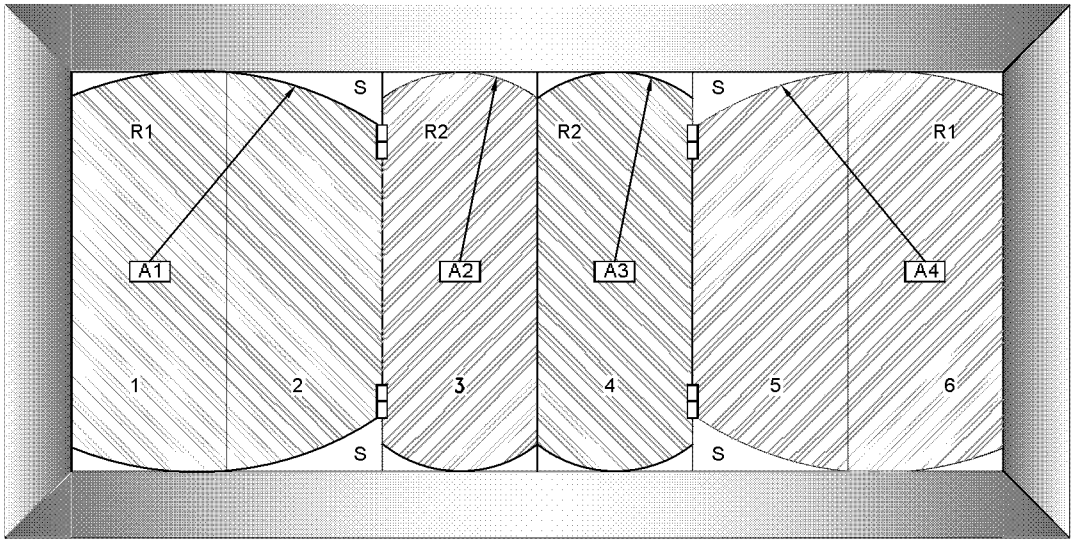
A2.1- Извещатель охранный магнитоконтактный (магнит)

A2.2- Извещатель охранный магнитоконтактный (геркон)

Все охранные извещатели устанавливаются внутри металлического шкафа

Приложение 11

Схема установки извещателя охранного поверхностного вибрационного многопозиционного для охраны немонолитной (многосекционной) конструкции



A1-A4 - многофункциональный вибрационный извещатель

R1- радиус действия для элементов конструкций 1,2 и 5,6, имеющих жесткую связь для передачи вибрации при разрушении

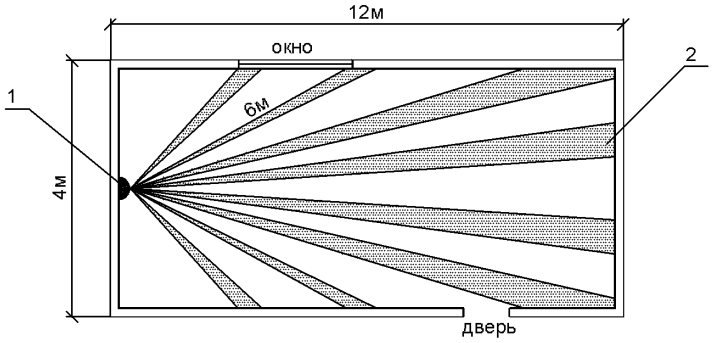
R2- радиус действия для элементов конструкций 3 и 4, не имеющих связи для передачи вибрации при разрушении

S - площадь, не охваченная радиусом R1 или R2($S < 0{,}1 м^2$)

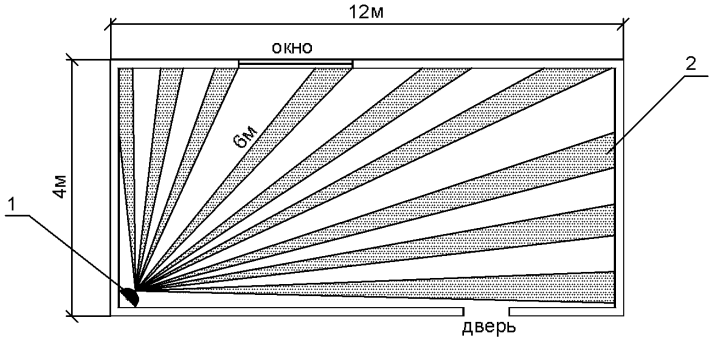
Приложение 12

Схема установки извещателя охранного объемного совмещенного (ИК+АК)

Установка на боковой стене



Установка в углу



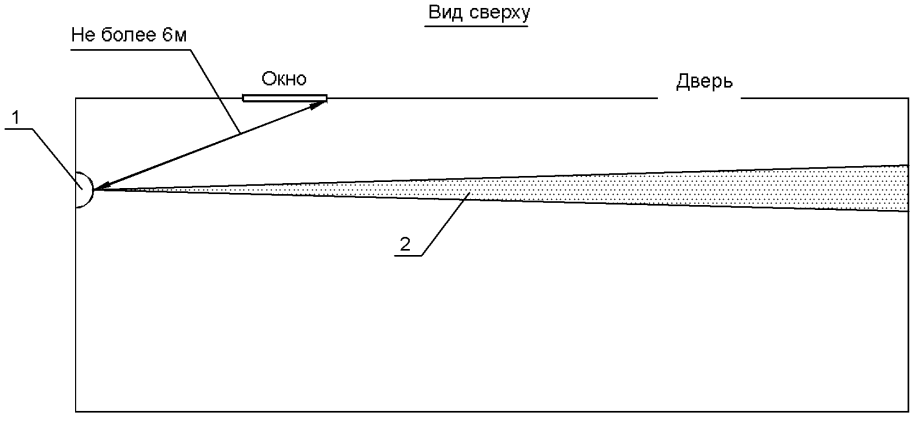
1- Извещатель охранный объемный совмещенный

2- Зона обнаружения

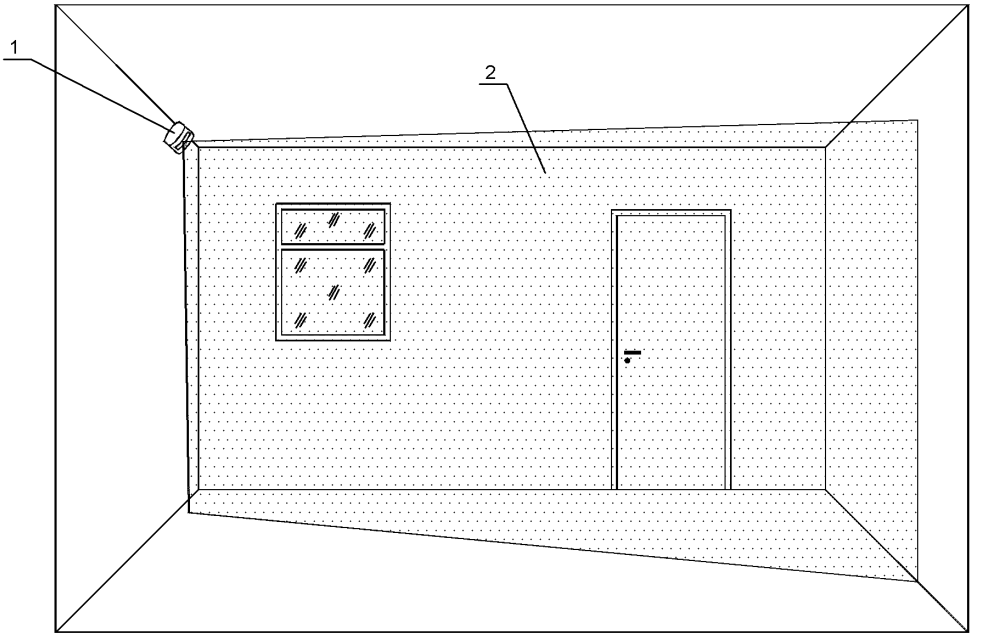
Приложение 13

Схема установки извещателя охранного поверхностного совмещенного (ИК+АК)

Вид сверху



Вид с боку

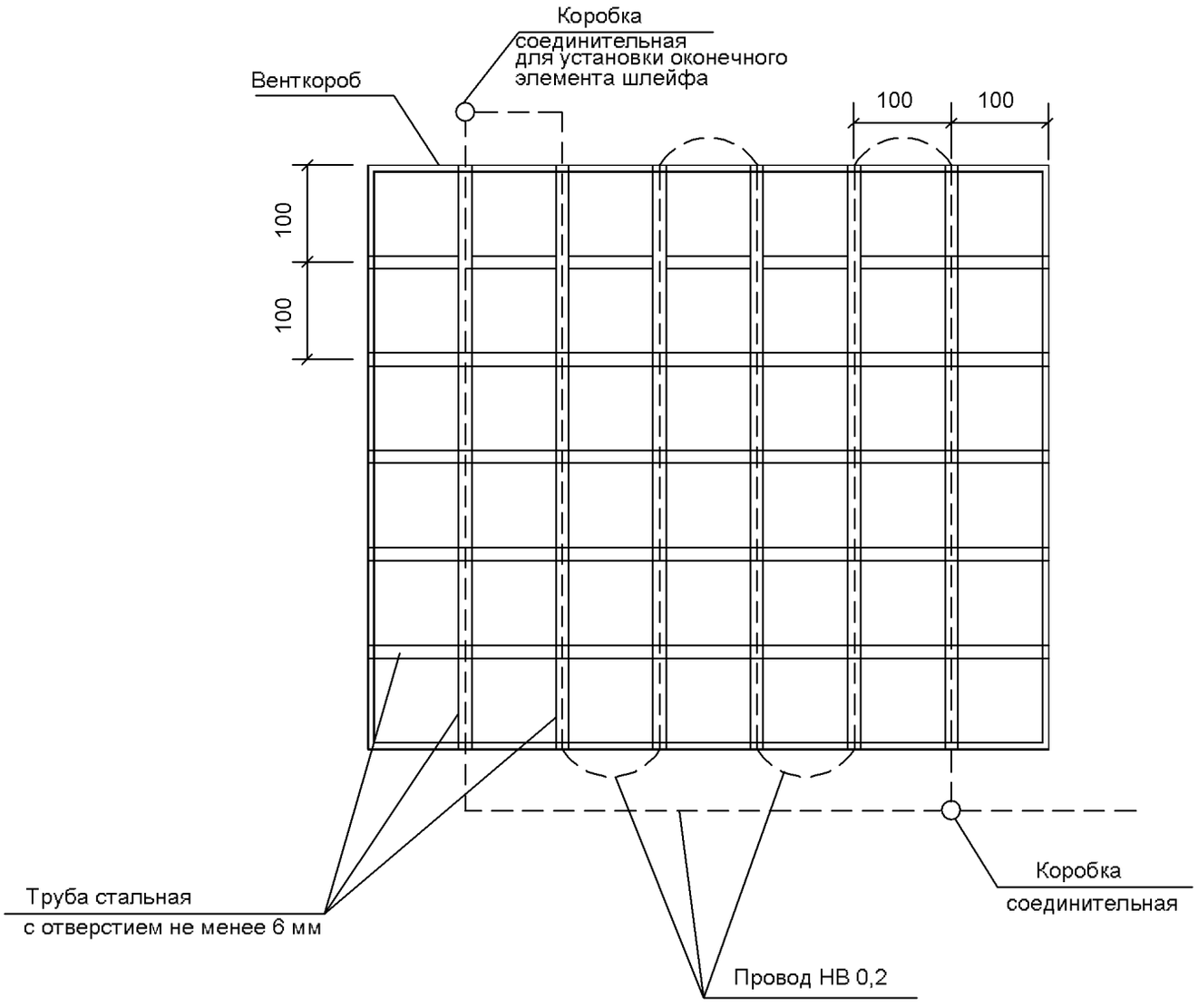


1- Извещатель охранный поверхностный совмещенный (ИК+АК).

2- Зона обнаружения ИК канала.

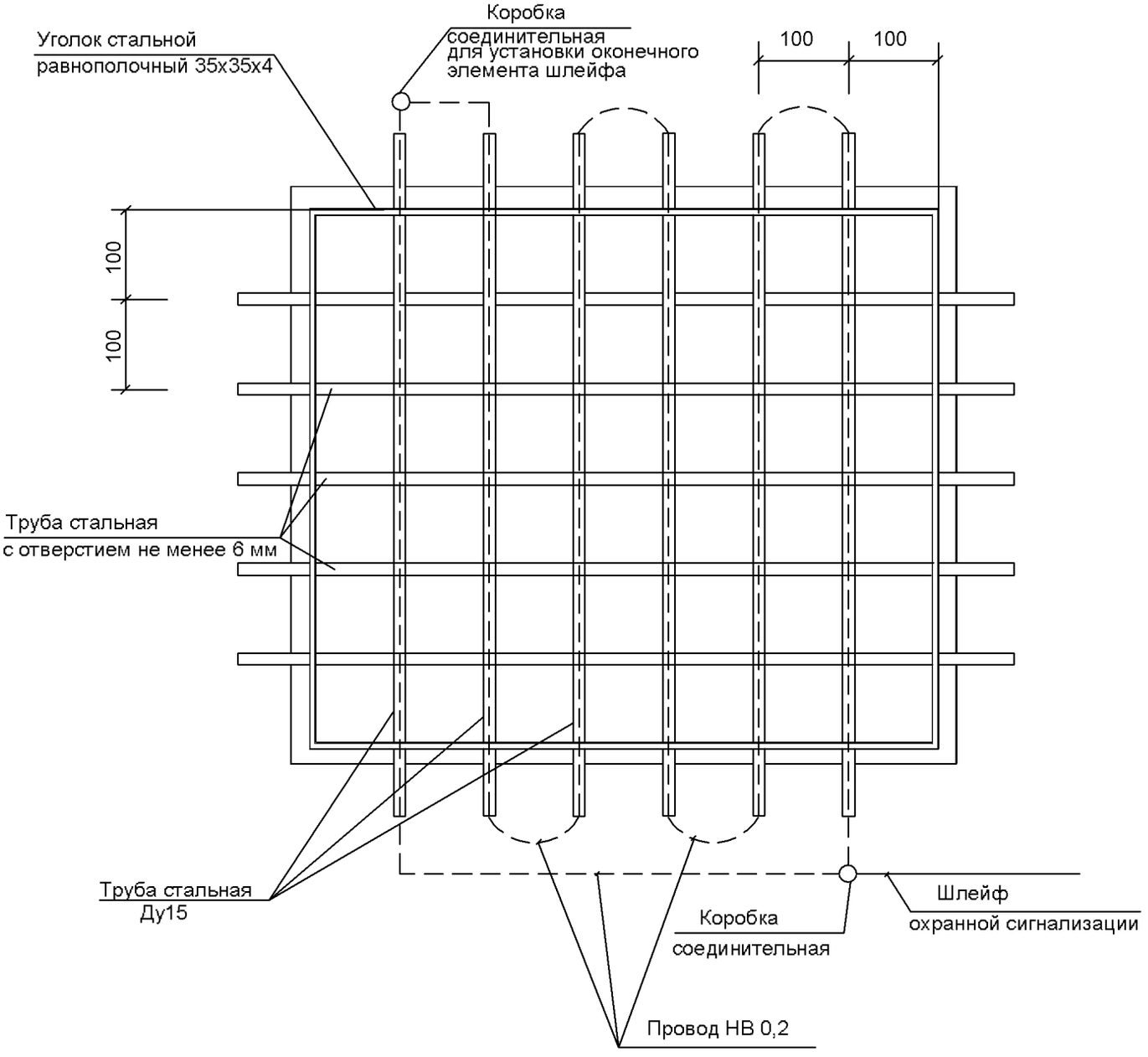
Приложение 14

Схема блокировки венткороба
омическим извещателем



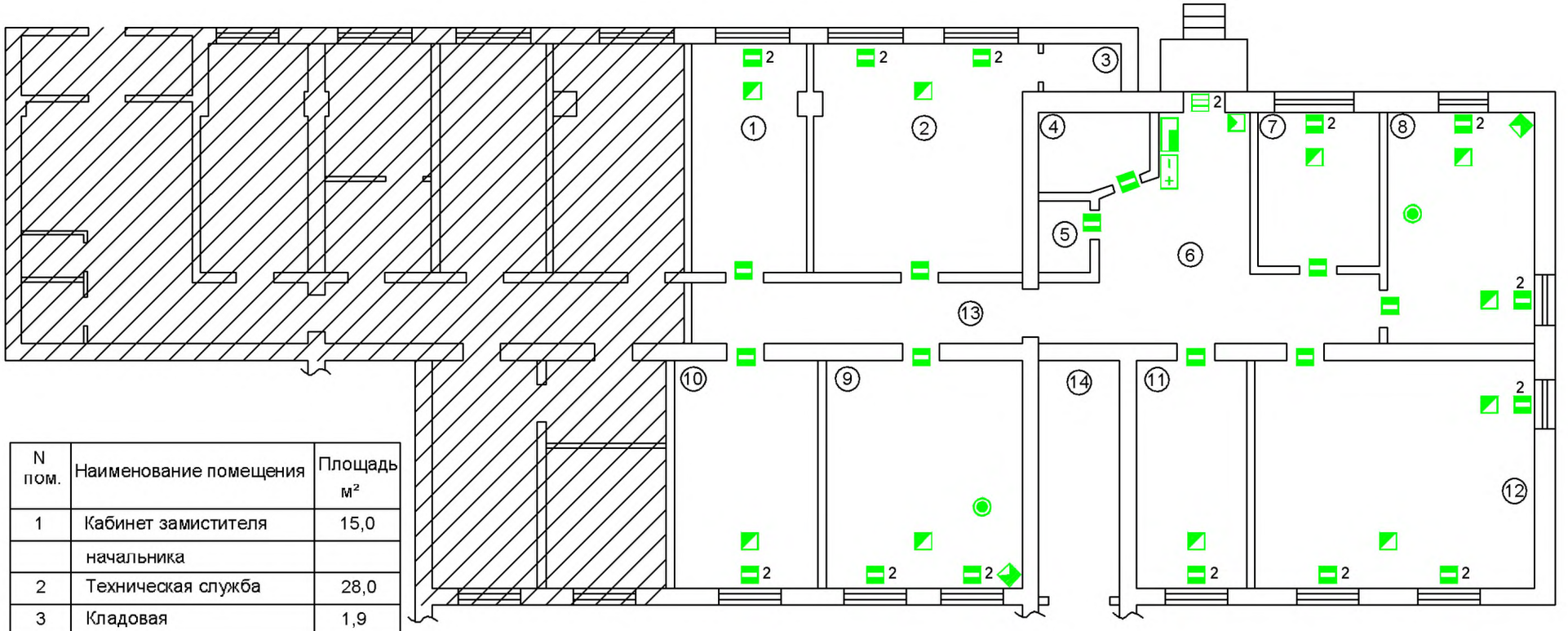
Приложение 15

Схема блокировки окна
омическим извещателем.



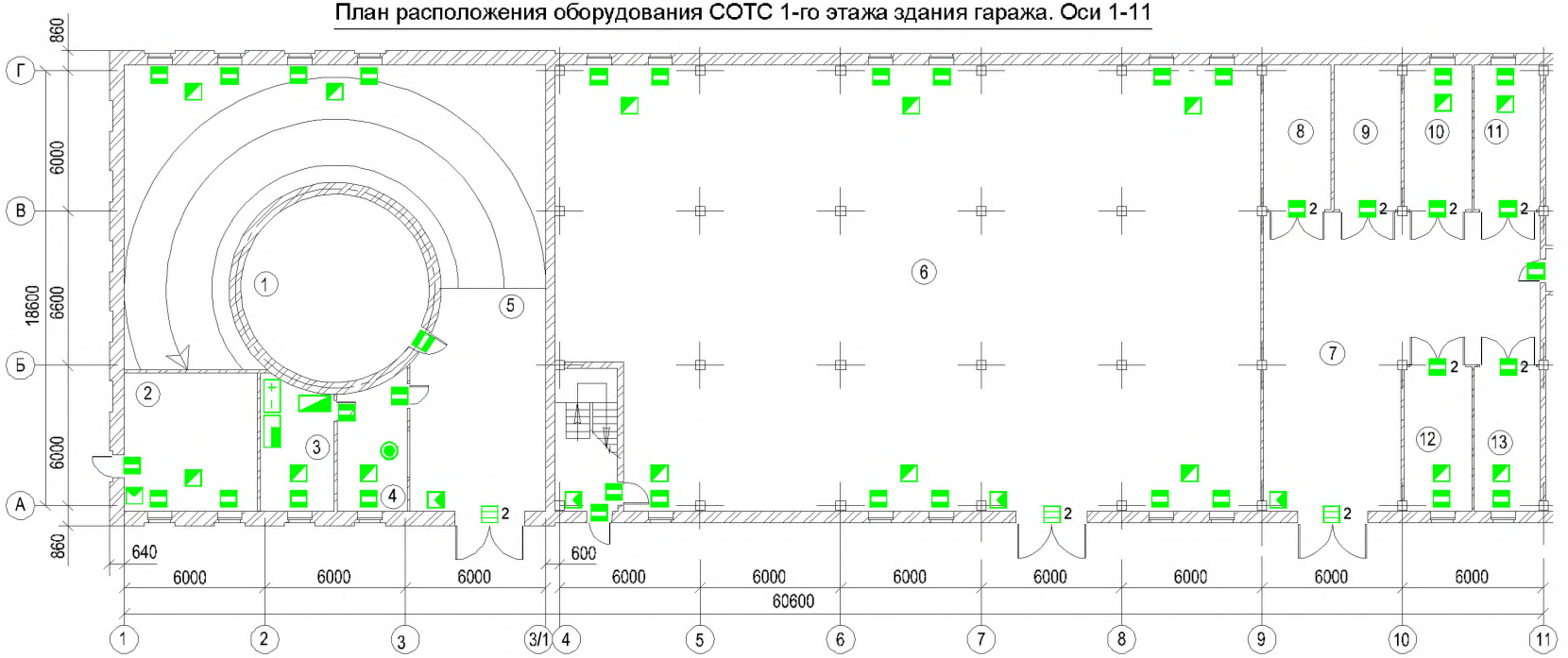
Приложение 16

План расположения оборудования СОТС УВО



N пом.	Наименование помещения	Площадь м²
1	Кабинет замистителя	15,0
	начальника	
2	Техническая служба	28,0
3	Кладовая	1,9
4	Склад	4,9
5	С/у	2,5
6	Коридор	23,3
7	Канцелярия	11,0
8	Кабинет начальника	19,5
9	Бухгалтерия	26,0
10	Отдел кадров	19,1
11	Правовая группа	14,6
12	Служебное помещение	37,2
13	Коридор	11,2
14	Подъезд жилого дома	

План расположения оборудования СОТС 1-го этажа здания гаража. Оси 1-11

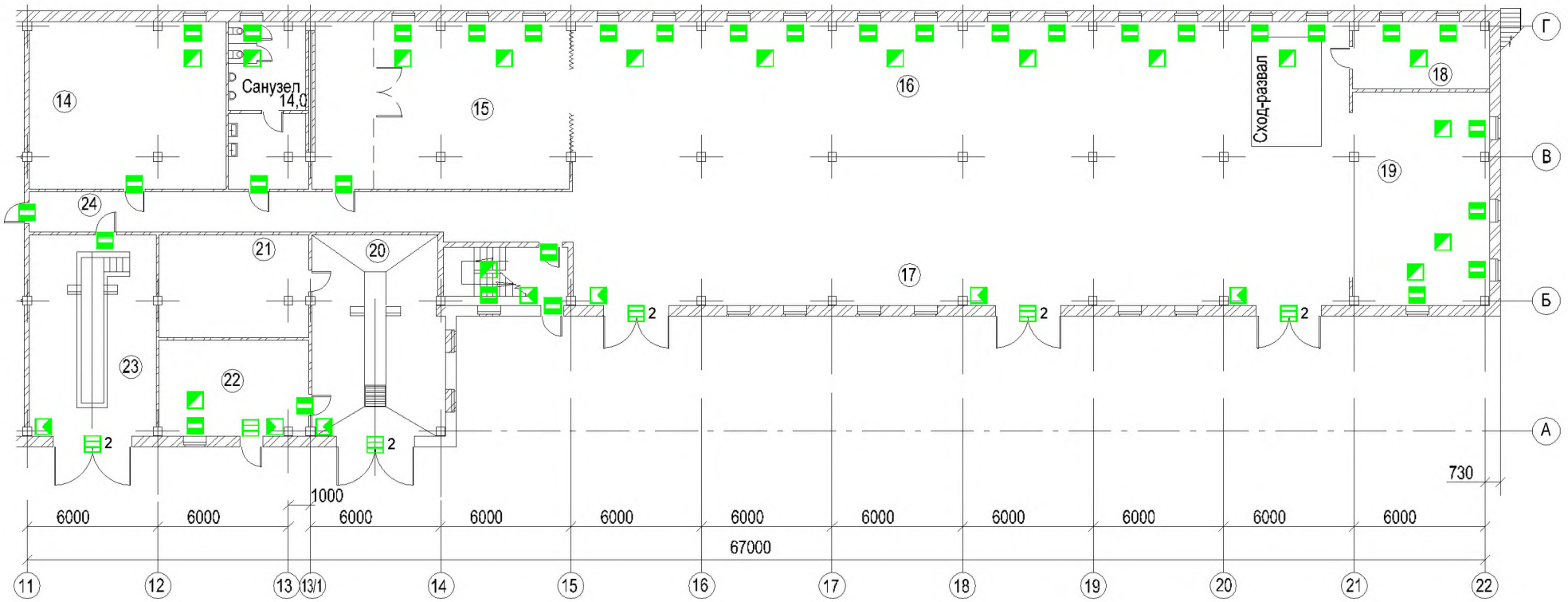


N пом.	Наименование	Площадь м²
1	Насосная	50,7
2	Насосная	20,6
3	Электростанция	17
4	Помещение охраны	16,1
5	Рампа	278,7
6	Гараж	551,6

7	Тамбур	113,4
8	Бокс 1	17,6
9	Бокс 2	17,6
10	Бокс 3	17,6
11	Бокс 4	17,6
12	Бокс 5	17,6
13	Бокс 6	17,6

Приложение 18

План расположения оборудования СОТС 1-го этажа здания гаража. Оси 11-22

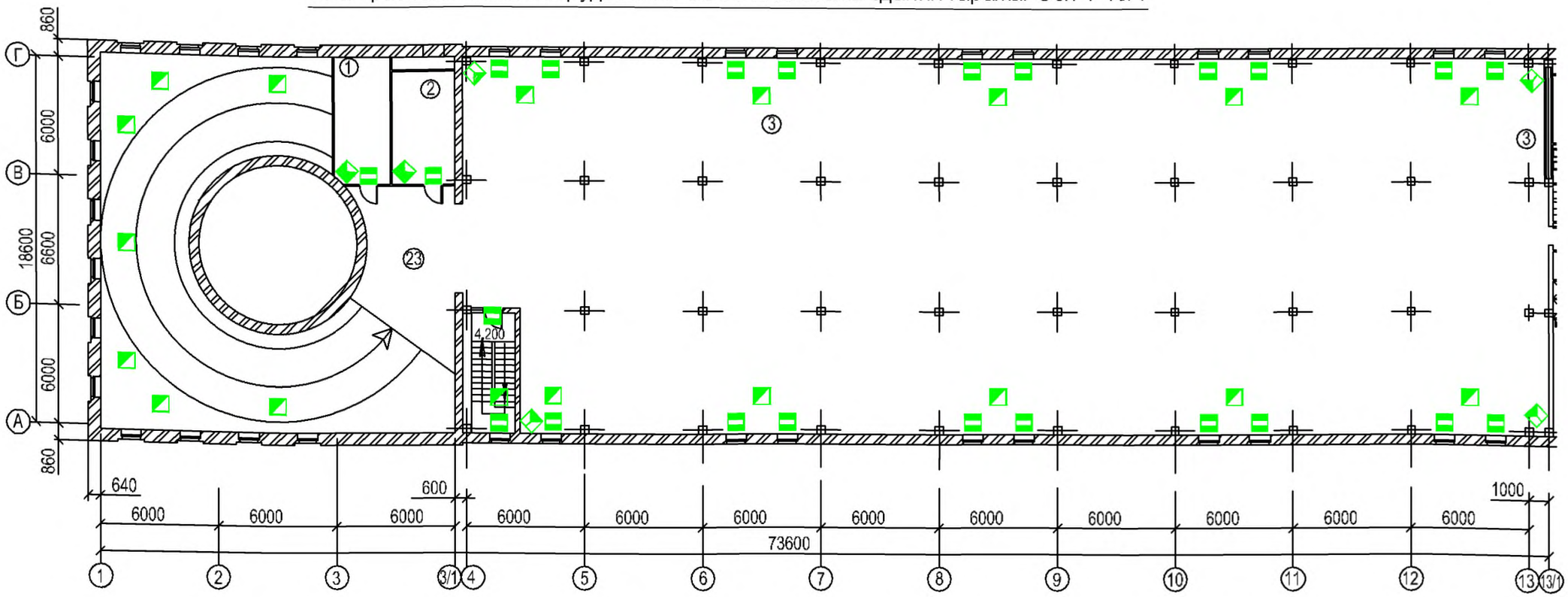


N пом.	Наименование	Площадь м²
14	Рем.участок	69,1
15	Уч-к кузовных работ	90,2
16	Участок ТО и ТР	463,5
17	Ремонтная зона	
18	Зарядная	19,1
19	Рем.участок	60,5

20	Мойка	58
21	Очистные сооружения	32,3
22	Шиномонтаж	29,9
23	Ремонт грузовых а/м	55,8
24	Коридор	48,9

Приложение 19

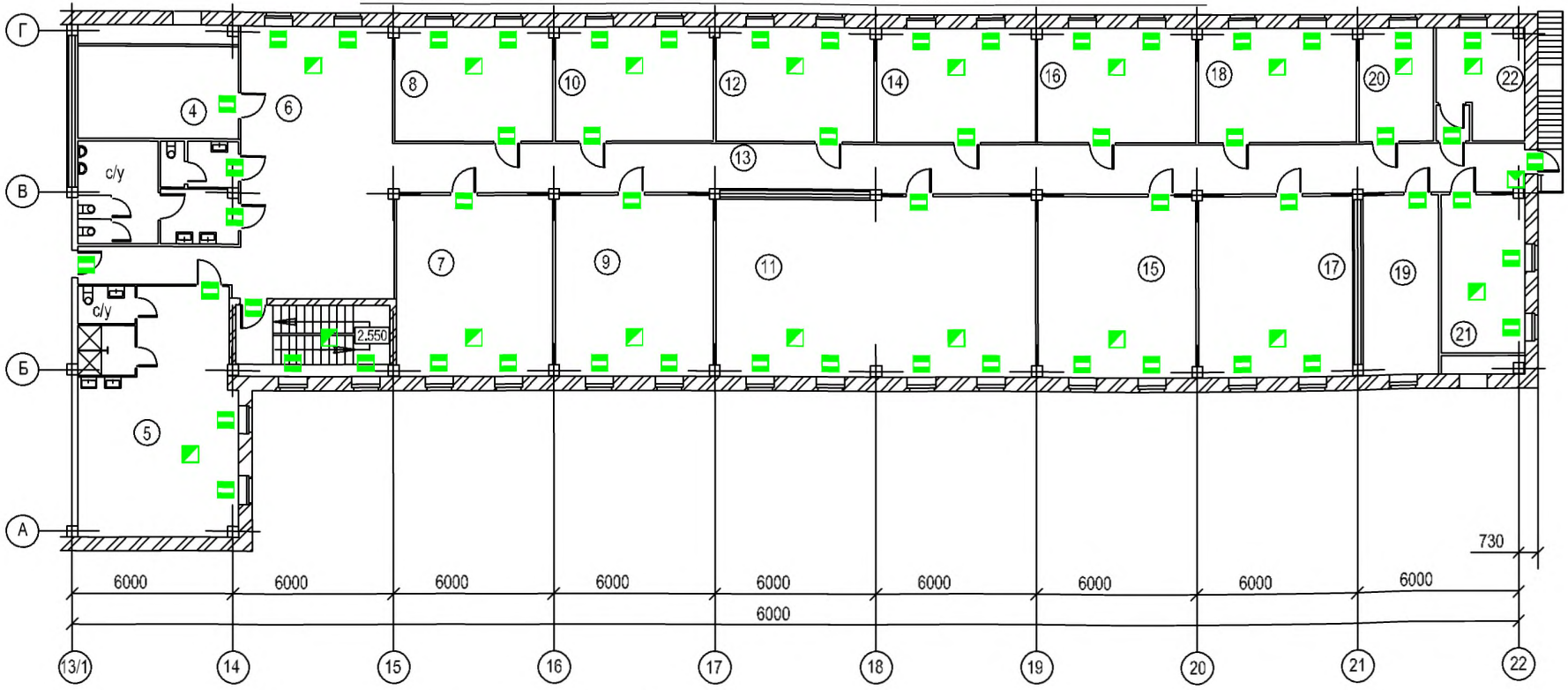
План расположения оборудования СОТС 2-го этажа здания гаража. Оси 1-13/1



N пом.	Наименование	Площадь м²
1	Вспомогательное пом.	18,1
2	Венткамера	20,6
3	Гараж	1024,9
23	Рампа	

Приложение 20

План расположения оборудования СОТС 2-го этажа здания гаража. Оси 13/1-22



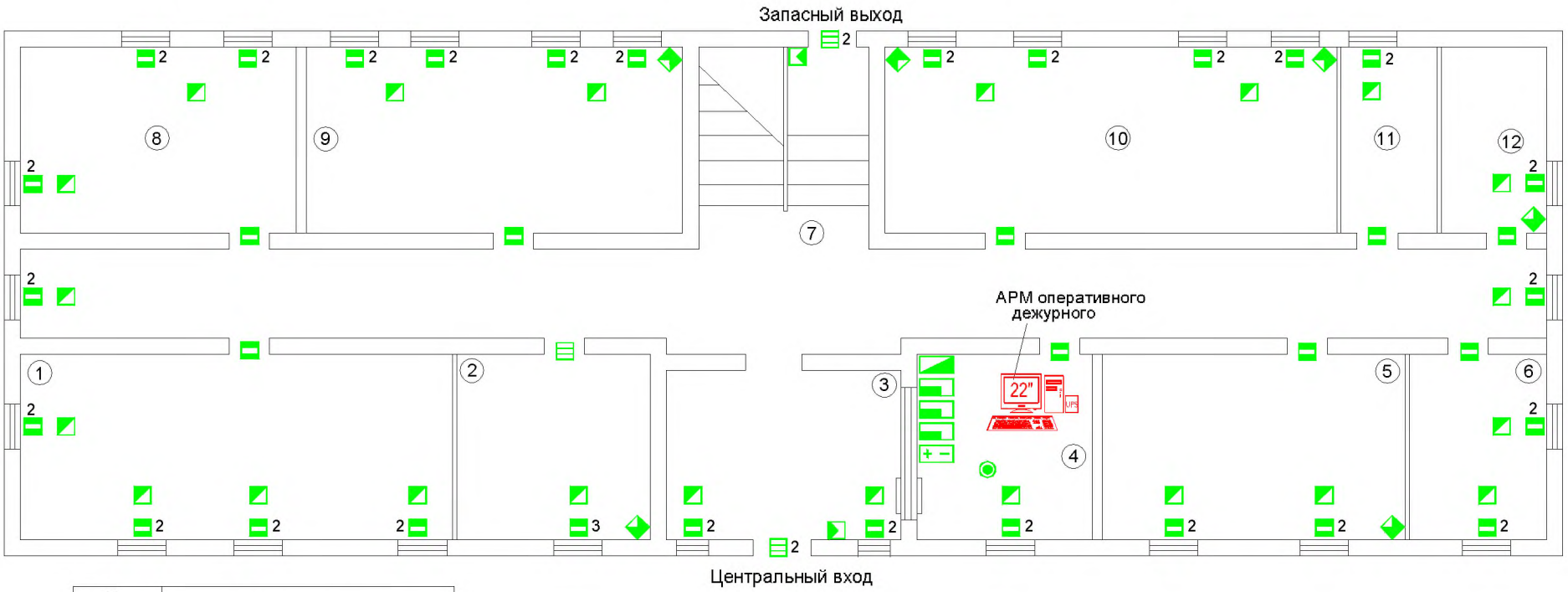
N пом.	Наименование	Площадь м²
4	Венткамера	25,2
5	Бытовое пом.	46,9
6	Холл	65,6
7	Склад зап.частей	39,3
8	Склад зап.частей	25,2
9	Служебное пом.	39,7
10	Служебное пом.	25,2

11	Комната отдыха водителей	79.2
12	Служебое пом.	25,2
13	Коридор	75,6
14	Служебое пом.	25,2
15	Комната приема пищи	39,7
16	Служебное пом.	25,2
17	Служебное пом.	38,7
18	Кладовая	25,2
19	Служебное пом.	19,1

20	Служебное пом.	11.8
21	Венткамера	20,4
22	Венткамера	13.8

Приложение 21

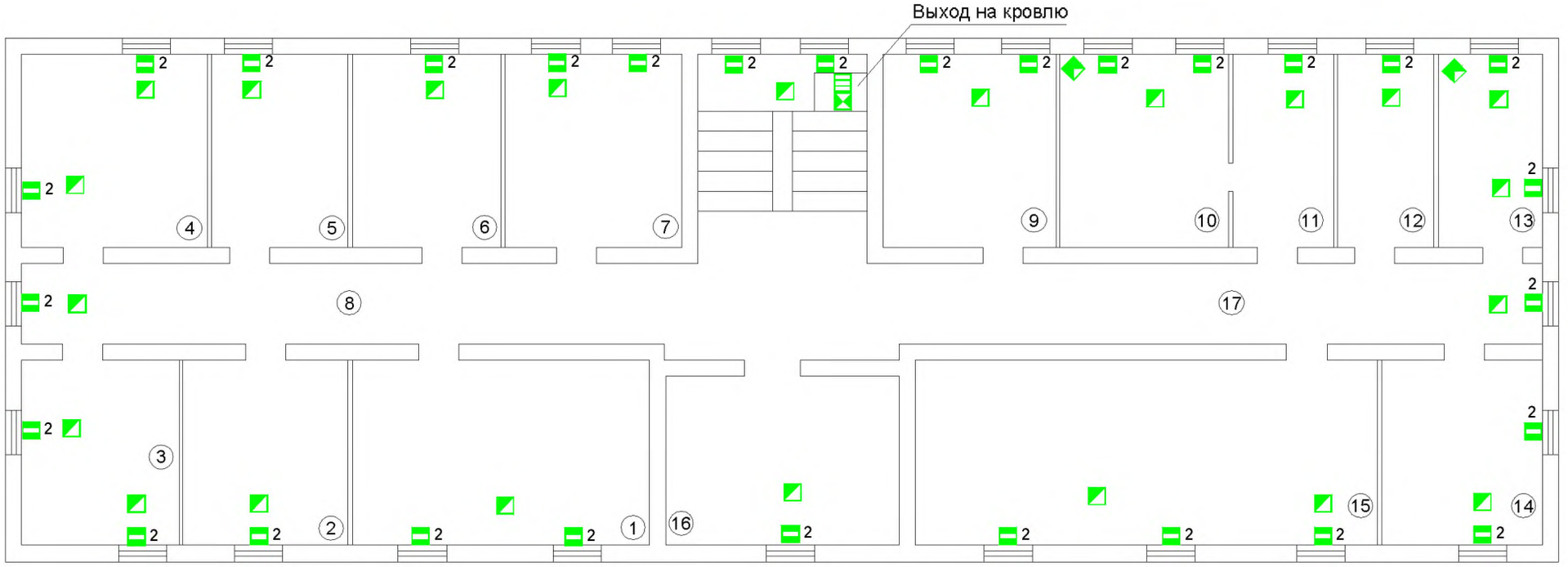
План расположения оборудования СОТС 1-го этажа здания ОВД



N п/п	Наименование
1	Актовый зал
2	Секретка (спец. помещение)
3	Холл
4	Помещение охраны
5	Секретариат
6	Кабинет
7	Коридор
8	Кабинет
9	Кабинет
10	Архив
11	Сан.узел мужской
12	Сан.узел женский

Приложение 22

План расположения оборудования СОТС 2-го этажа здания ОВД



N п/п	Наименование	N п/п	Наименование
1	Кабинет	10	Кабинет начальника
2	Кабинет	11	Приемная
3	Кабинет	12	Кабинет
4	Кабинет	13	Спецпомещение
5	Кабинет	14	Кабинет
6	Группа кадров	15	Учебный класс
7	Группа кадров	16	Кабинет
8	Коридор	17	Коридор
9	Юристконсульт		

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к третьей категории»

Система охранной сигнализации внешнего периметра объекта

РАЗДЕЛ 2

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	60
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	62
3.	СИСТЕМА ОХРАННОЙ СИГНАЛИЗАЦИИ (СОС) ВНЕШНЕГО ПЕРИМЕТРА ОБЪЕКТА	62
3.1	Типы и виды СОС. Их назначение и функции	62
3.2	Критерии и принципы выбора СОС	86
3.3	Размещение и монтаж СОС	88
3.4	Система тревожной сигнализации	90
3.5	Организация передачи информации о срабатывании сигнализации	91
3.6	Система передачи извещений (СПИ)	91
3.7	Прокладка проводов, кабелей	91
3.8	Электропитание	91

ПРИЛОЖЕНИЯ

Приложение 1	Схема блокировки калитки вибрационным и магнитоконтактным извещателями.	94
Приложение 2	Схема блокировки ограждения от перелаза инфракрасным линейным извещателем.	95
Приложение 3	Пример защиты ограждения в два рубежа охраны радиоволновым и инфракрасным линейными извещателями.	96
Приложение 4	Схема монтажа извещателя охранного линейного радиоволнового.	97
Приложение 5	Варианты блокировки ограждения вибрационным извещателем.	98
Приложение 6	Схема блокировки ограждения ёмкостным извещателем.	99
Приложение 7	Схема блокировки от проникновения через здание вибрационным извещателем.	100
Приложение 8	Схема блокировки ворот инфракрасным линейным извещателем от перелаза и на открывание магнитоконтактным извещателем.	101
Приложение 9	Схема блокировки ворот вибрационным и магнитоконтактным извещателями.	102
Приложение 10	Схема блокировки сетчатого ограждения проводноволновым извещателем.	103
Приложение 11	Схема блокировки на перелаз через здание проводноволновым извещателем.	104
Приложение 12	Схема блокировки сплошного ограждения от перелаза проводноволновым извещателем (вид 1).	105

Приложение 13	Схема блокировки сплошного ограждения от перелаза проводноволновым извещателем (вид 2).	106
Приложение 14	Схема блокировки ворот радиоволновым линейным и магнитоконтактным извещателями.	107
Приложение 15	Схема установки радиолокационной станции с фиксированным углом обзора на столбе.	108
Приложение 16	Здание КПП.	109

1. ОБЩАЯ ЧАСТЬ

Методические рекомендации по оснащению ведомственных объектов СОС разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 2.01.2013 № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;

- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- Р 78.36.017-2012 «Об эффективном применении запирающих устройств, имеющихся на отечественном рынке, при организации охраны имущества граждан и организаций. Методические рекомендации»;
- Р 78.36.019-2012 «Рекомендации по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий»;
- Р 78.36.026-2012 «Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны ограждённых территорий и открытых площадок»;
- Р 78.36.028-2012 «Рекомендации. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов»;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану. Методические рекомендации»;
- Р 78.36.032-2013 «Инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1. Объекты»;
- Р 78.36.034-2013 «Мониторинг применения и сравнительный анализ испытаний различных видов периметрового ограждения (основного ограждения, дополнительного ограждения, предупредительного внешнего и внутреннего ограждения). Классификация»;
- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения»;
- Р 78.36.050-2015 «Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних

периметров, дверей, окон, витрин и подступов к отдельным предметам»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ – Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

В соответствии с пунктом 4.3 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом III категории по степени потенциальной угрозы понимается отдельно стоящие здания или сооружения, имеющие прилегающую территорию (или без таковой), на которых осуществление круглосуточного пропускного режима и круглосуточного дежурства не обязательно.

Объект: отдельно стоящее здание, с прилегающей территорией, на котором осуществление круглосуточного ПР и круглосуточного дежурства не обязательно.

Ограждение прилегающей территории имеется.

Инженерно-техническая укреплённость ограждения территории и помещений соответствует III категории.

Помещения полиции, отнесённые к III категории, должны быть оборудованы техническими средствами охраны (далее ТСО):
- системой охранно-тревожной сигнализации;
- системой охранной сигнализации внешнего периметра объекта;
- системой охранной телевизионной;
- системой контроля и управления доступом.

3. СИСТЕМА ОХРАННОЙ СИГНАЛИЗАЦИИ ВНЕШНЕГО ПЕРИМЕТРА ОБЪЕКТА

3.1 Типы и виды СОС. Их назначение и функции.

1. Сейсмические средства обнаружения.

Сейсмические извещатели реагируют на колебания или деформацию контактирующей с ними среды, вызванные перемещением людей. Чувствительный элемент (ЧЭ) извещателя устанавливается непосредственно

в грунт и преобразует микроперемещение грунта в электрический сигнал ЧЭ, который анализируется в блоке обработки сигналов (БОС).

В вибрационном или сейсмическом извещателе используется одинаковый преобразователь физических величин в электрический сигнал. Например, вибрационный кабель, установленный на бетонном ограждении или в грунте, полностью определяет назначение прибора – для обнаружения пролома или подкопа.

Структура построения включает в себя выносную линейную часть и цифровой комплект отображения информации. Выносная часть предназначена для приёма сейсмических сигналов, их предварительного усиления и передачи в цифровой комплекс. В состав выносной части входят сейсмические датчики, предварительные усилители, блоки питания, магистральные кабели.

Такие системы способны обеспечить обнаружение, пеленгацию, классификацию и восстановление траектории движения в полосе шириной от 30 до 70 м от осевой линии охраняемой зоны.

Применение сейсмических средств обнаружения.

Различная установка ЧЭ обеспечивает возможность охранять подступы к периметру, обнаруживать попытку подкопа под ограждением, а также охранять неогороженный рубеж.

По сравнению с другими средствами обнаружения сейсмические извещатели имеют два главных преимущества:

- скрытый, маскируемый ЧЭ визуально не обнаруживает рубеж охраны, а пассивный принцип действия исключает возможность его обнаружения по акустическим и электромагнитным полям, что фактически сравнивает шансы подготовленного и неподготовленного нарушителей;

- высокая вероятность обнаружения при перемещении нарушителя ползком или при попытке подкопа.

Сейсмические средства обнаружения с вибрационным кабелем.

В извещателях в качестве ЧЭ используется вибрационный кабель (Рисунок 1).

ЧЭ извещателя может устанавливаться под любыми видами ограждений. Используется фланговое включение ЧЭ, симметрично от места установки блока электронного.

К недостаткам этих извещателей можно отнести возможность выдачи ложной тревоги:

- при перемещении корней деревьев, которые при сильных порывах ветра могут вызывать колебания почвы;

- от воздействия индустриальных помех, прежде всего в городской зоне, где располагаются такие источники сейсмических помех, как автомобильный и железнодорожный транспорт, аэропорты, промышленные предприятия, хозяйственные коммуникации и т.д.;

- при резких перепадах температуры природной среды, при замерзании или оттаивании грунта, подвижках грунта.

Главным недостатком этих извещателей является уменьшение чувствительности при промерзании грунта больше глубины установки виброкабеля.

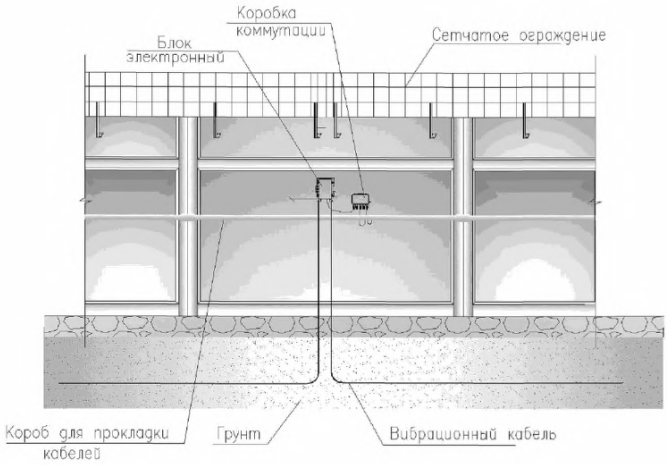


Рисунок 1. Установка ЧЭ для обнаружения подкопа.

Сейсмические средства обнаружения с геофонами.

Применение в качестве ЧЭ сейсмических датчиков – геофонов повышает чувствительность извещателей. Геофон является более сложным и дорогим устройством по сравнению с вибрационным кабелем. Конструкция геофона представлена на рисунке 2.

Геофон представляет собой проводящую обмотку и помещённый внутрь неё магнитный сердечник, который может свободно колебаться вдоль оси обмотки. При колебании магнита в катушке наводится напряжение, регистрируемое анализатором.



Рисунок 2. Геофон.

Геофоны могут устанавливаться на ограждении. Монтаж на «жёстком» ограждении позволяет обнаруживать нарушителя, преодолевающего массивную бетонную или кирпичную стену.

В некоторых случаях геофоны устанавливают под землёй, но крепят их к основаниям стен (Рисунок 3, грунт с геофона снят). Такая конструкция позволяет обнаруживать нарушителя как вблизи периметра, так и при попытках преодолеть стену.



Рисунок 3. Геофон под землёй на кирпичной стене.

Геофоны монтируют под землёй на глубине от 15 до 35 см на расстоянии от 2 до 4 м друг от друга. Рекомендуется устанавливать сенсоры в стабильный и плотный грунт.

Охранная система состоит из двух основных компонентов: процессора и кабельного шлейфа с подключёнными к нему геофонами. Сенсоры регистрируют вибрации, создаваемые проходящим человеком, и посылают сигналы на анализатор для обработки.

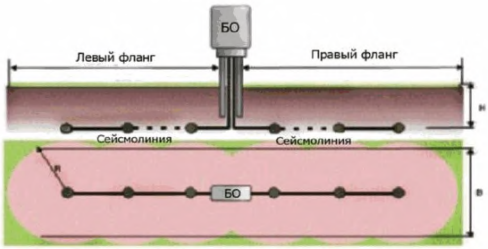


Рисунок 4. Размещение геофонов.

Установленный под землёй геофон позволяет уверенно обнаруживать сигнал от идущего человека на расстоянии от 1,5 до 2,0 м, поэтому геофоны монтируют вдоль периметра на расстоянии 3,0 м друг от друга.

Однако, эти же геофоны будут регистрировать движение транспорта или перемещение корней деревьев при ветровых порывах на расстоянии нескольких десятков метров (Рисунок 5).

2. Манометрические средства обнаружения.

Извещатель предназначен для блокирования территорий объектов по периметру и обнаружения нарушителя при взаимодействии его с ЧЭ. Он обеспечивает создание зон обнаружения с использованием ЧЭ манометрического типа.

Конструкция и принцип действия извещателя с ЧЭ манометрического типа представляет собой электронный сенсор и подключённые к нему специальные шланги, заполненные жидкостью (антифризом), которые укладываются в землю на глубину от 0,25 до 0,3 м на расстоянии от 1,0 до 1,5 м друг от друга. При прохождении чувствительной зоны нарушитель создаёт определённое давление на грунт. Шланги, в свою очередь, обнаруживают, а сенсор измеряет дифференциальное изменение давления между ними. На рисунке 7 показано воздействие человека на шланги.

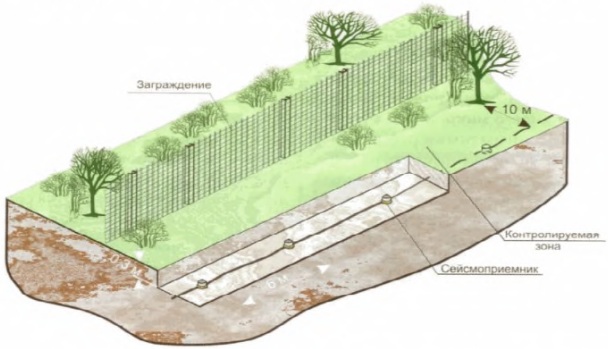


Рисунок 5. Расположение геофонов среди растительности.

В состав линейной части извещателя, устанавливаемой в грунт, кроме шлангов и сенсора входят компенсационные клапаны, которые обеспечивают компенсацию давления в шлангах. В сенсоре размещаются высокочувствительные мембраны и микропроцессор для преобразования и анализа сигналов.

Шланги (трубы) изготавливаются из специальной композиции синтетических материалов, обеспечивающих необходимую эластичность и долговечность при нахождении в грунте.

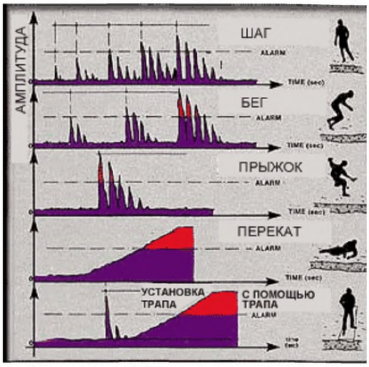


Рисунок 6. Характерные сигналы.



Рисунок 7. Воздействие человека на шланги.

Достоинства этого извещателя:

1. Учитывая, что ЧЭ устанавливается под землёй, асфальтом или бетоном, извещатель в большей степени подходит для объектов, где требуется определённая устойчивость к атмосферным и электромагнитным воздействиям, строгое соблюдение правил пожаро- и взрывобезопасности.

2. Извещатель обеспечивает надёжное обнаружение нарушителей при пересечении чувствительной зоны шагом, бегом, прыжками, перекатыванием, с использованием трапов, досок или путём подкопа. На рисунке 6 показаны характерные сигналы при различных перемещениях нарушителя.

Установка извещателя:

Шланги благодаря их гибкости могут быть уложены в грунт произвольным способом, что делает практически невозможным определение охраняемой зоны нарушителем. Кроме того, благодаря этим качествам, появляется уникальная возможность установки извещателя на периметрах со сложной конфигурацией и рельефом, без специальной подготовки и обслуживания зон обнаружения.

Однако высокая чувствительность датчиков требует, чтобы деревья и крупные кустарники находились не ближе 3 – 4 м от шлангов.

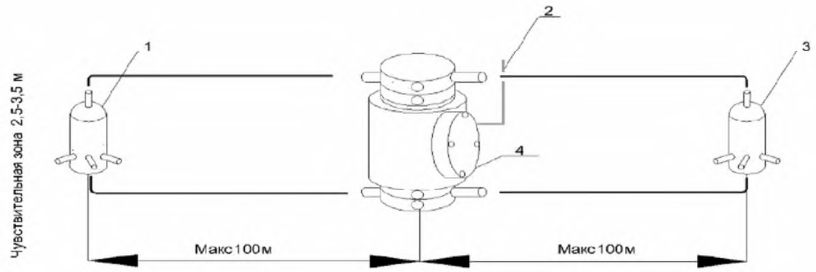


Рисунок 8. Двухтрубная версия, где 1, 3 – компенсационные клапаны, 2 – подземный кабель к блоку управления, 4 – сенсор.

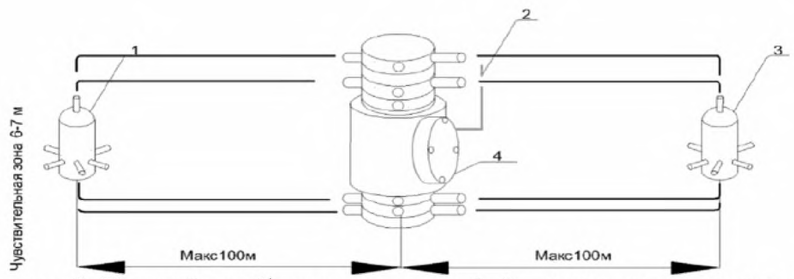


Рисунок 9. Четырёхтрубная версия, где 1, 3 – компенсационные клапаны, 2 – подземный кабель к блоку управления, 4 – двойной сенсор.



Рисунок 10. Установка чувствительного элемента (шлангов).

Недостатками манометрических извещателей являются большой объём подготовительных и монтажных работ при установке линейной части, сложность эксплуатации, особенно при замене ЧЭ, высокая стоимость.

Извещатель обеспечивает надёжное обнаружение нарушителей при пересечении чувствительной зоны шагом, бегом, прыжками, перекатыванием, с использованием трапов, досок или путём подкопа и является идеальным решением (в большинстве случаев) для защиты внешнего периметра.

3. Ёмкостные средства обнаружения.

К достоинствам ёмкостных извещателей относятся отсутствие «мёртвых» зон и высокая чувствительность. Зона обнаружения легко настраивается и регулируется.

Извещатель состоит из ЧЭ и блока обработки (БО). Извещатели выдают извещение о тревоге при приближении нарушителя или касании им ЧЭ и хорошо работают на периметре со сложной конфигурацией и рельефом.



Рисунок 11. Установка ЧЭ на железобетонном заборе.

ЧЭ этих извещателей представляет собой один или несколько металлических электродов, укреплённых на изоляторах вдоль или сверху ограждения, и является, по сути, антенной системой. На рисунке 11 показана установка на бетонном ограждении ЧЭ в виде проводников на пластмассовых изоляторах. Когда нарушитель приближается к электродам или касается их, ёмкость антенной системы изменяется, что регистрируется в БО, выдаётся извещение о тревоге.

Также достоинством этих извещателей является использование инженерного ограждения в качестве ЧЭ.

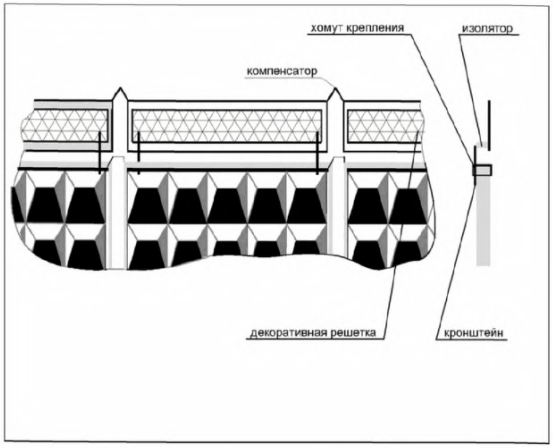


Рисунок 12. Декоративная решётка в качестве ЧЭ.



Рисунок 13. Инженерное оборудование периметра.

На рисунке 12 показана декоративная решётка в качестве ЧЭ, установленная по верху ограждения. Однако, необходимо помнить, что ЧЭ этих извещателей должен быть изолирован от земли.

На рисунке 13 показано оборудование периметра реального объекта с помощью железобетонного забора с козырьком из металлической сварной сетки, установленной на металлических уголках, изолированных от полотна ограждения и являющихся ЧЭ извещателя. На рисунке также показаны внутреннее и внешнее ограждения.

Дестабилизирующие факторы, влияющие на работу ёмкостных средств обнаружения:

1. Воздействие вредных, «паразитных» сигналов от большого количества внешних помех.

Природа их возникновения может быть самой разнообразной:

- метеоосадки (дождь, снег, гололёд, туман, гроза, ветер и т.д.);
- индустриальные помехи - электрические и радионаводки, вибрации, акустический шум.

2. Воздействие птиц при посадке на ЧЭ.

3. Влияние растительности в ближней зоне ЧЭ или при непосредственном его касании.

4. Сложность определения полезного сигнала на фоне помех.

Все эти источники помех и некоторые другие могут вызывать ложные тревоги.

Современные ёмкостные извещатели частично или полностью защищены от перечисленных помех и выдают ложные тревоги только при экстремальных условиях.



Рисунок 14. Пример установки РЛСО.

4. Радиоволновые средства обнаружения.

Радиоволновые (РВСО) и радиоволновые линейные (РЛСО) средства обнаружения получили широкое распространение при защите периметров объектов.

В зависимости от принципа действия различают активные или пассивные РВСО и РЛСО.

Пассивные РВСО и РЛСО используют собственное излучение объекта обнаружения или вызываемое им изменение электромагнитных полей (ЭМП) внешних источников (как правило, вещательных теле- и радиостанций).

Активные РВСО и РЛСО используют собственные ЭМП для формирования зоны обнаружения.

Различают одно- и двухпозиционные РВСО и РЛСО. Однопозиционные имеют общий блок приёмопередатчика (пассивные РВСО и РЛСО всегда являются однопозиционными), двухпозиционные имеют разнесённые блоки передатчика и приёмника.

Пассивные РЛСО применяются для обнаружения нарушителей, имеющих собственное электромагнитное излучение. Например, нарушителя, имеющего на руках какое-либо электрооборудование, использующего микроробота, малоразмерный летательный аппарат и т.д.

Активные однопозиционные РЛСО включают в себя:

- однопозиционную радиолокационную станцию (РЛС);
- нелинейный радиолокатор;
- однопозиционное микроволновое СО.

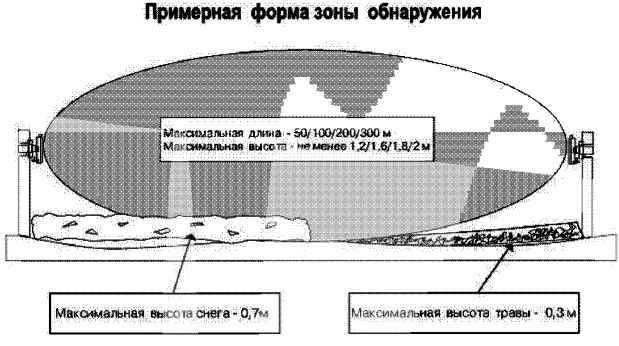


Рисунок 15. Примерная зона обнаружения двухпозиционного РЛСО.

5. Вибрационные (трибоэлектрические) средства обнаружения.

Вибрационные извещатели устанавливаются на «мягкие» заграждения из металлической сетки, колючей проволоки, армированной колючей ленты (АКЛ) (Рисунок 16).



Рисунок 16. Установка извещателя на АКЛ.

Извещатели обнаруживают нарушителя при перелазе, разрушении или демонтаже полотна ограждения.

В качестве ЧЭ используются специальные кабели со спиралевидным центральным проводником (типа КТВ). Также широко применяются телефонные экранированные кабели (типа ТПП10×2×0,5), обладающие выраженным «паразитным» трибоэффектом.

К достоинствам этих извещателей также относятся небольшая потребляемая мощность (до 500 мВт) и расширенный температурный диапазон эксплуатации (от минус 50 до плюс 65 °С).

К тактическим достоинствам вибрационных извещателей можно отнести:

1. Возможность установки ЧЭ с учётом геометрии защищаемого периметра.

Величина угла поворота ограничена лишь допустимым радиусом изгиба самого ЧЭ.

2. Размеры зоны обнаружения ограничены размерами контролируемого ограждения.

Недостатки и ограничения.

1. Высокие требования, предъявляемые к качеству монтажа как самого ограждения, так и ЧЭ (крепёж кабеля к ограждению, монтаж соединительных муфт и т.д.).

2. Необходимость регулярного контроля параметров настройки извещателя, так как свойства ограждения могут заметно изменяться при резких изменениях температуры, а также при смене сезонов.

3. Недопустимость прямого контакта ЧЭ с ветвями деревьев и больших кустарников.

4. Возможность выдачи ложной тревоги при проезде тяжёлой техники вдоль ограждения и от ударов по нему камнем, палкой и т.д.

5. Ограниченность применения. Извещатели могут применяться только на «мягких» (сетчатых) или на лёгких металлических ограждениях (профнастил, гофрированный лист). Установка этих извещателей на

«жёстких» ограждениях (железобетонных, кирпичных или конструкциях из пластика) не предусмотрена.

Техническим решением охраны для таких ограждений является устройство дополнительных козырьков из металлической сетки или спирали из армированной колючей ленты.

Извещатели с диапазоном акустических частот (виброакустические).

Вибрационный кабель позволяет определять разрушение полотна способами перепиливания и перекусывания.

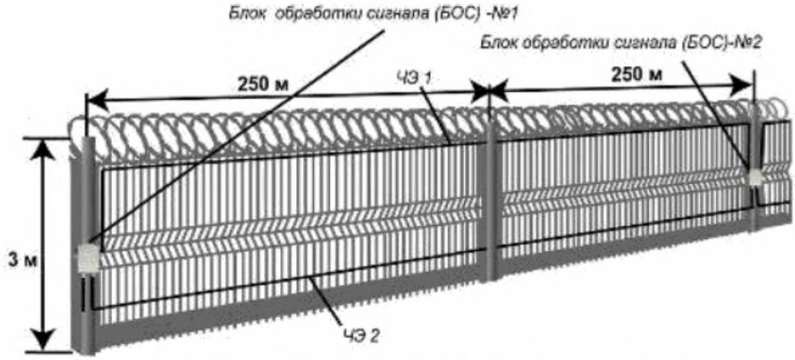


Рисунок 17. Вариант защиты вибрационным кабелем от перелаза и разрушения ограждения.

В отличие от остальных, извещатели с диапазоном акустических частот работают даже на «жёстких» (тяжёлых) сварных решётках и на качественных деревянных ограждениях, так как акустические волны распространяются в ограждении при любом способе преодоления или воздействия (Рисунок 18).

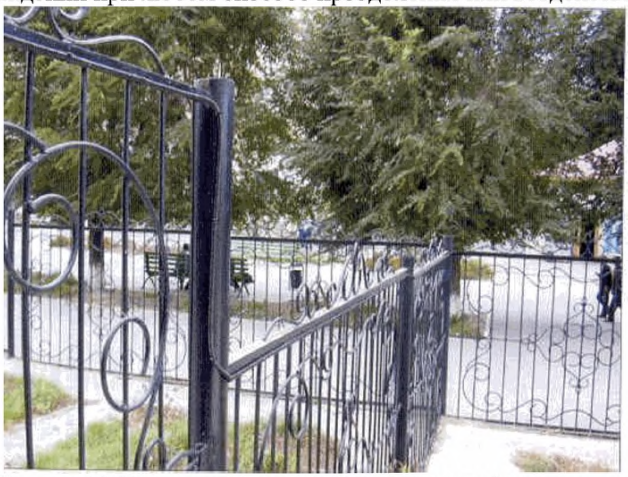


Рисунок 18. Установка извещателя на сварных решётках.

Виброакустические извещатели могут устанавливаться на различные существующие ограждения (Рисунок 19).



Рисунок 19. Ограждения с виброакустическими извещателями.

6. Оптико-электронные средства обнаружения (активные, пассивные, волоконно-оптические).

Оптико-электронные средства обнаружения (ОЭСО) построены на анализе оптического излучения. Они подразделяются на 2 типа: активные и пассивные. Активные регистрируют изменение собственного излучения, вызванное вторжением нарушителя в ЗО, пассивные регистрируют тепловое излучение нарушителя.

6.1 Активные ОЭСО.

Линейные оптико-электронные извещатели (активные инфракрасные (ИК) извещатели), как правило, имеют двухблочную конструкцию и состоят из блока излучателя (БИ) и блока фотоприёмника (БФ), образующих оптическую систему. Появление в зоне обнаружения (ЗО) извещателя оптически непрозрачного объекта вызывает прерывание ИК луча (или снижение его мощности), попадающего в приёмник, который формирует извещение о тревоге путём изменения сопротивления контактов, подключаемых к ШС. Также встречаются извещатели, имеющие одноблочную конструкцию, оптическая система которых состоит из излучателя и фотоприёмника, объединённых в одном корпусе, а также светоотражателя (катафота). Входные окна БИ и БФ обычно закрыты специальными фильтрами. Схема активного ИК извещателя представлена на рисунке 20.

Достоинством активных ИК извещателей является то, что их обнаружительная способность не зависит от характеристик теплового излучения человека (нарушителя). Также они нечувствительны к изменению характеристик теплового излучения окружающих объектов (фона) и возникающим тепловым помехам, что очень актуально при эксплуатации на открытых площадках.

К недостаткам активных ИК извещателей можно отнести их способность формировать только линейную ЗО, что обуславливает узкую область применения.

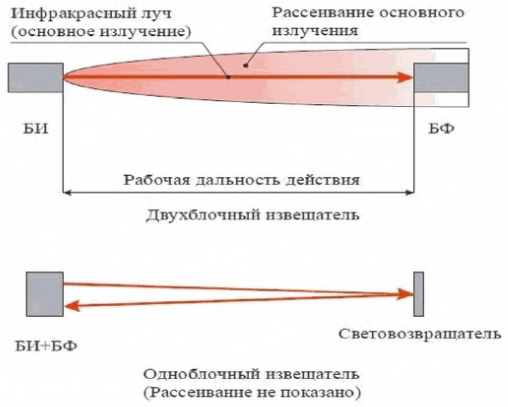


Рисунок 20. Схема активного ИК извещателя.

Отчасти эта проблема может быть решена путём организации поверхностной ЗО за счёт применения извещателей, формирующих несколько ИК лучей, или построения ИК барьера из нескольких извещателей (Рисунок 22).

Их можно применять для организации первого рубежа охраны объектов (блокировка протяженных инженерных ограждений (заборов), окон или дверей снаружи здания, ворот, вентиляционных шахт и каналов и т.п.). Охраняемые объекты должны быть прямолинейными, в противном случае, объект разбивается на несколько прямолинейных участков, для блокировки которых используется отдельный извещатель (Рисунки 21, 22).

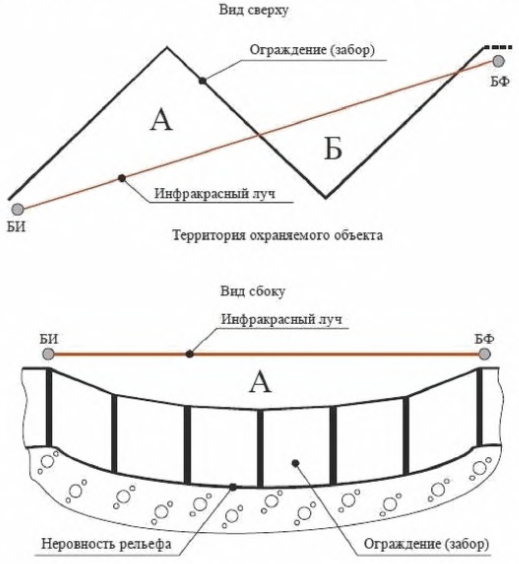


Рисунок 21. Неправильное использование активного ИК извещателя.

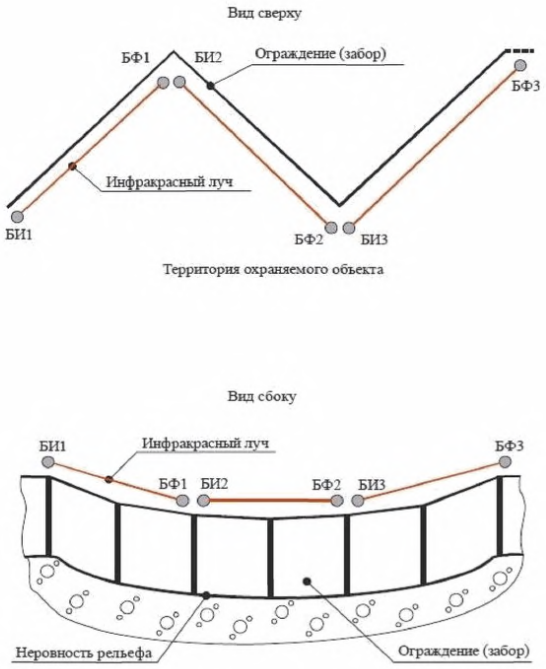


Рисунок 22. Схема охраны объекта сложной формы.

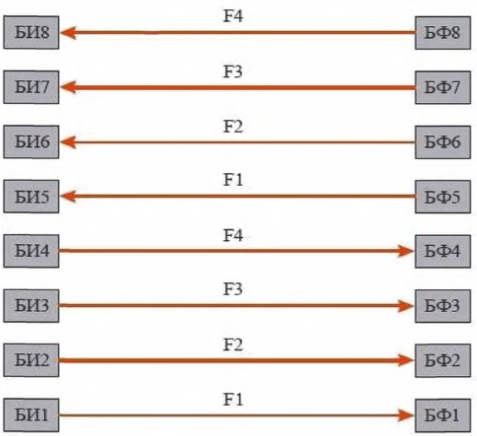


Рисунок 23. Пример барьера ИК извещателей, работающих на одной частоте.

При необходимости создания ИК барьера в горизонтальной плоскости извещатели необходимо устанавливать таким образом, чтобы излучения одной рабочей частоты близко расположенных БИ были разнонаправлены и не могли одновременно попадать на входное окно одного БФ (рисунок 24).

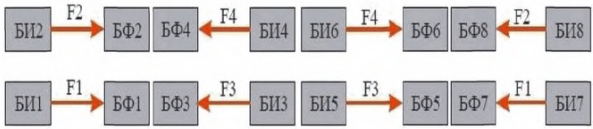


Рисунок 24. Пример ИК барьера в горизонтальной плоскости.

6.2 Пассивные оптико-электронные ИК извещатели.

Пассивные ИК извещатели, предназначенные для эксплуатации на открытом воздухе, разделяются по типу формируемой ЗО: объёмные, поверхностные и линейные.

Они предназначены для обнаружения нарушителя, перемещающегося в их ЗО.

7. Волоконно-оптические средства обнаружения.

По способу применения и определения нарушителя по физическому воздействию на ЧЭ волоконно-оптические системы (ВОС) аналогичны вибрационным извещателям. Однако ЧЭ этих систем по сравнению с обычными кабельными линиями обладают иными параметрами и потребительскими свойствами.

В волоконно-оптических охранных системах используются различные методы регистрации сигналов вторжения.

ЧЭ прочен, легок, гибок и прокладывается любыми способами (в трубах, на инженерных ограждениях, в земле).

К несомненным достоинствам волоконно-оптических систем следует отнести:

- их невосприимчивость к электромагнитным помехам, что позволяет использовать их в зонах с высоким уровнем таких помех;
- возможность их применения для защиты не только ограждений, но и неограждённых территорий;
- возможность организации охраны достаточно протяжённого периметра с конфигурацией практически любой сложности;
- высокая электробезопасность; зону обнаружения с этим ЧЭ можно организовать на взрывоопасных объектах, а также под водой (в пресной или морской среде);
- отсутствие излучения электромагнитной энергии (трудно обнаружить с помощью поисковой техники);
- возможность эксплуатации в неблагоприятных атмосферных условиях (морской туман, кислотные пары, индустриальные выбросы, песок) и в диапазоне температур от минус 30° до плюс 70° С. Оболочка ЧЭ обеспечивает защиту оптоволокна от УФ излучения, влаги и т.п.

К недостаткам волоконно-оптических систем следует отнести:

- высокую стоимость работ при укладке ЧЭ в грунт;

- необходимость использования ЧЭ в оболочке при установке на ограждении, что повышает стоимость системы;

- сложность процедуры сращивания и ремонта ЧЭ в полевых условиях (требуется применение дорогостоящего устройства для сварки волокон);

- отстройка от помех приводит к тому, что система способна обнаруживать только «силовые» вторжения, сопровождающиеся значительными механическими воздействиями;

- потерю чувствительности при промерзании грунта;

- усложнение аппаратуры ВОС для локализации места нарушения с достаточной точностью.

Варианты установки волоконно-оптического кабеля представлены на рисунках 25-28.

8. Проводноволновые средства обнаружения.

В большинстве случаев ЧЭ проводноволновых извещателей является пара расположенных параллельно проводников, к которым подключены соответственно передатчик и приемник радиосигналов.

Достоинством проводноволновых извещателей является независимость зоны обнаружения от профиля почвы и точное следование линии ограждения.

Другим достоинством этих извещателей является простота и небольшая стоимость ЧЭ. В качестве проводников ЧЭ используется провод полевой телефонной связи П-274М, который обеспечивает достаточную механическую прочность и стойкость к атмосферным воздействиям.



Рисунок 25. Вариант монтажа ВОС на металлическом заборе.



Рисунок 26. Бетонный забор с АКЛ.



Рисунок 27. Установка ЧЭ на АКЛ.



Рисунок 28. Установка ЧЭ на кованом заборе.

Зона обнаружения.

Передатчик формирует импульсный высокочастотный сигнал, создающий электромагнитное поле между проводниками. Вокруг проводящей пары («открытой антенны») образуется объёмная чувствительная зона с поперечным сечением в виде эллипса, в фокусах которого расположены проводники. Расстояние между проводниками обычно составляет 0,4 м, при этом зона обнаружения имеет размер 0,5×0,8 м.

При появлении нарушителя в зоне обнаружения сигнал на входе приёмника изменяется, извещатель формирует извещение о тревоге.

ЧЭ устанавливают в основном двумя способами: на консолях по верху ограждения (рисунок 29) либо на изоляторах, непосредственно на ограждении.

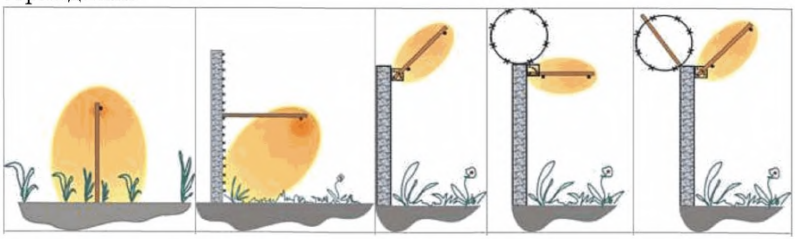


Рисунок 29. Установка ЧЭ проводноволновых извещателей.



Рисунок 30. Варианты установки ЧЭ.

Недостатком такой установки ЧЭ извещателей является возможность выдачи ложной тревоги от вибрации проводов. Поэтому извещатели устанавливают на любых «жёстких» ограждениях (кирпич, бетон, металл), так как вибрация проводов на «мягких» ограждениях может привести к выдаче ложной тревоги.

Существует другой вариант установки проводноволновых извещателей – верхний провод устанавливают на диэлектрических стойках по верху ограждения на высоте от 1,5 до 2,0 м, а нижний прокладывают по земле или углубляют в грунт от 0,03 до 0,05 м. Ширина зоны обнаружения на грунте составляет 3,0 м.

Извещатель ЛВВ - «линия вытекающей волны».

ЧЭ извещателя представляет собой перфорированный кабель, в котором внешний проводник не обеспечивает полного экранирования центрального проводника, и определенная часть энергии передаваемого высокочастотного сигнала излучается через отверстия во внешнюю среду, часть энергии проникает в приёмный кабель такой же конструкции (Рисунок 31).

В передающем кабеле устанавливается режим, близкий к режиму бегущей волны, а в приёмном кабеле наводится опорный сигнал.

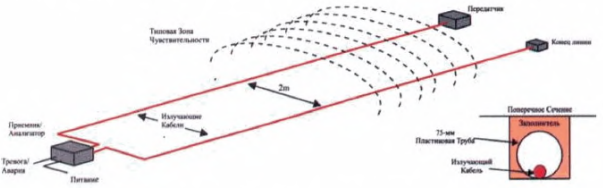


Рисунок 31. ЛВВ – извещатель.

Принцип действия ЛВВ основан на регистрации возмущения электромагнитного поля при пересечении нарушителем объёмной зоны обнаружения. Отраженная от нарушителя электромагнитная волна принимается приёмным кабелем, вследствие чего происходит низкочастотная модуляция амплитуды и фазы опорного сигнала.

Кабели ЧЭ могут устанавливаться на ограждение и закапываться в грунт.

Ширина зоны обнаружения зависит от чувствительности кабеля (вида его конструкции), частоты сигнала, расстояния между кабелями, параметров подстилающей поверхности, способа обработки сигнала. Высота зоны обнаружения может достигать 1,5 м.

Типовая зона обнаружения при установке кабелей ЧЭ извещателя на кирпичной стене показана на рисунке 32.

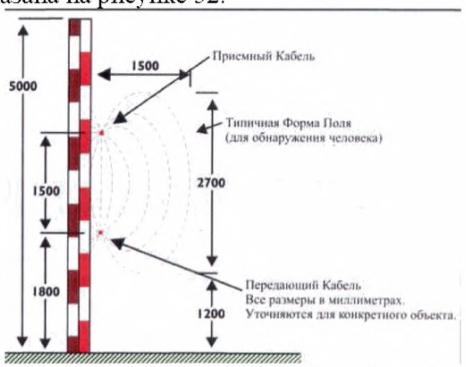


Рисунок 32. Типовая зона обнаружения при установке ЧЭ на стене.

Из рисунка 33 видно, что допускается наличие отдельных кустов и деревьев в непосредственной близости к ЧЭ.



Рисунок 33. Установка ЧЭ на кирпичной стене.

8. Средства обнаружения и охранные комплексы на основе радиолокационных станций.

Радиолокационные системы (РЛС) предназначены для круглосуточного мониторинга обстановки на объектах с малой и большой протяжённости периметра территории.

Задачами РЛС по охране периметра и территории объектов являются:

- обнаружение движущихся целей;
- измерение дальности, азимута и радиальной скорости целей;
- распознавание классов целей (человек, группа людей, автомобиль);
- идентификация и автосопровождение целей;
- автоматическое построение радиолокационной карты охраняемой территории, неподвижных объектов, а также посторонних (вновь появившихся) и движущихся целей;
- привязка радиолокационной карты к топографической карте местности.

РЛС могут выступать в качестве целеуказателей для поворотных видео и тепловизионных камер. В этом случае РЛС решают задачу обнаружения, оценки скорости и класса движущейся цели на расстоянии, существенно превышающем то, с которым работают видеокамеры, а камеры и тепловизоры осуществляют детальное видеонаблюдение обнаруженной цели.

РЛС отвечает за измерение скорости движения цели, определяет её класс и начинает вести слежение, фокусируя на неё камеры видеонаблюдения (тепловизор).

Информация отображается в виде координатной сетки со схематическим отображением на ней стационарных объектов, а также местоположения всех обнаруженных целей.

По каждой из целей показывается класс цели, её координаты и скорость передвижения в данный момент. Кроме того, можно выполнить привязку информации с РЛС к топографической карте местности.

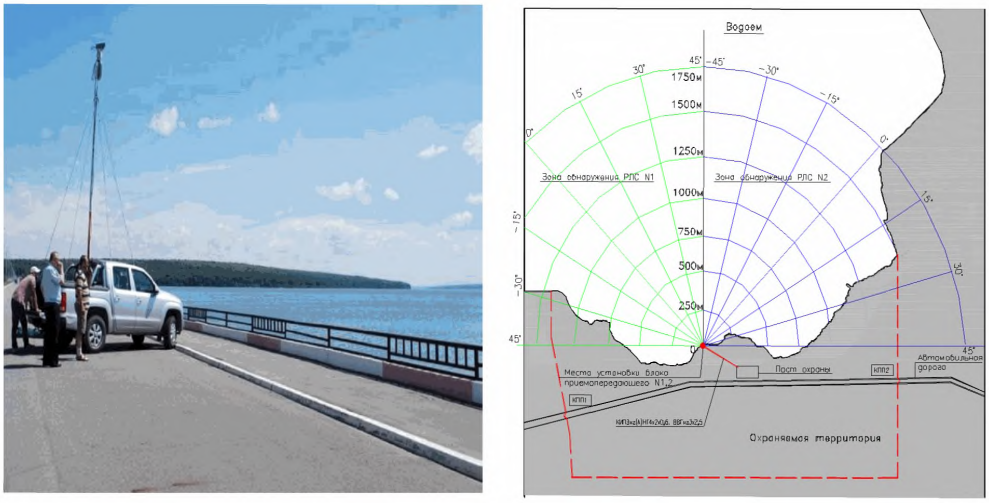


Рисунок 34. Привязка радиолокационной карты к топографической карте местности.



Рисунок 35. РЛС с круговым углом обзора и камера видеонаблюдения (тепловизор).

9. Комбинированные и совмещённые средства обнаружения.

Для построения эффективной защиты периметра используют несколько рубежей и датчики, работающие на различных физических принципах. Это

позволяет обнаружить достоверное проникновение на охраняемый объект и уменьшить количество ложных срабатываний сигнализации. Достоинством таких извещателей является возможность одновременного обнаружения попыток проникновения нарушителя на охраняемый объект различными способами.



Рисунок 36. РЛС с фиксированным углом обзора и камера видеонаблюдения (тепловизор).

3.2 Критерии и принципы выбора СОС.

ТСО периметра должны выбираться в зависимости от вида предполагаемой угрозы объекту и условий эксплуатации.

Все компоненты СОС должны удовлетворять следующим требованиям:

- поддерживать круглосуточный режим функционирования (допускается проведение профилактических работ по поддержанию оборудования систем в рабочем состоянии без прекращения функционирования системы);
- функционировать в автоматическом режиме;
- включать средства самодиагностирования;
- соответствовать российским и международным стандартам;
- учитывать возможность для расширения как функциональных, так и количественных характеристик систем;
- обеспечивать бесперебойное электропитание СОС;
- обеспечивать защиту информации при передаче от периферийных узлов на пульт дежурного от несанкционированного внешнего доступа и копирования;
- все компоненты инженерных и технических средств безопасности должны быть функционально взаимоувязаны в интегрированную систему безопасности.

При выборе технических средств охранной сигнализации для охраны периметра территории и открытых площадок с материальными ценностями необходимо учитывать:

- вид предполагаемой угрозы объекту;

- помеховую обстановку (высоковольтные ЛЭП, радиостанции, мощные электроустановки, электрифицированный транспорт);
- рельеф местности;
- место расположения объекта (внутри населенного пункта или нет, примыкающие строения);
- протяжённость периметра;
- инженерно-техническую укреплённость периметра;
- тип ограждения;
- наличие автомобильных и пешеходных дорог вдоль периметра;
- зоны отторжения и их ширину;
- климатические условия: температура (в России: от - 60 до + 60 °С), влажность, туман, дождь, гроза, снег, град, наледь, ветер, пыль, песок, солнечная радиация;
- назначение и функции, выполняемые техническими средствами охранной сигнализации.

В качестве ТСО акватории могут использоваться ТСО, применяемые при оборудовании периметров территории: средства сигнализации (извещатели радиолучевые или радиоволновые, гидроакустические приборы, магнитометрические системы обнаружения), сигнальные фонари и ракеты, прожекторы, радио- и проводные средства связи, средства наблюдения (зрительные трубы, бинокли, приборы ночного видения, стационарные, мобильные и портативные тепловизоры) и громкоговорящие радиоустановки (электромегафоны, усилители).

В зависимости от категории объекта МВД определяется, какой должна быть рубежность охраны (однорубежная или многорубежная).

3.3 Размещение и монтаж СОС.

3.3.1 Для объектов МВД III-й категории охрана объекта должна быть однорубежной.

ТСО периметра размещаются на ограждениях, зданиях, строениях, сооружениях в зоне отторжения, на стенах, специальных столбах или стойках, обеспечивающих отсутствие колебаний и вибраций.

Периметр, с входящими в него воротами и калитками, следует разделять на отдельные охраняемые участки (зоны) с подключением их отдельными шлейфами сигнализации к прибору приёмно-контрольному малой ёмкости или к пульту внутренней охраны, установленному на контрольно пропускном пункте (КПП) или в специально выделенном помещении 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 на тревожное извещение.

Основные ворота, устанавливаемые, как правило, около КПП или постоянного поста полиции, должны выделяться в самостоятельный участок периметра, шлейф сигнализации которого подключается на отдельный номер пульта внутренней охраны и отключается на время пропуска транспорта. Запасные ворота, калитки должны входить в тот участок периметра, на котором они находятся, и включаться в шлейф сигнализации этого участка.

Все входы в помещение КПП, а также управляемые преграждающие конструкции оборудуются замковыми устройствами и средствами ОС, которые выдают сигнал тревоги при попытке преодоления нарушителем этих конструкций путём их вскрытия и разрушения.

Ограждение транспортного КПП, калитки в нём, а также основные и вспомогательные ворота оборудуются замковыми устройствами и средствами ОС, калитки, кроме этого, запирающими устройствами и средствами постовой телефонной связи.

В качестве пультов внутренней охраны могут использоваться приёмно-контрольные приборы (ППК) средней и большой ёмкости (концентраторы), системы передачи извещений, автоматизированные системы передачи извещений, радиосистемы передачи извещений, интегрированные системы.

При блокировке периметра извещателями с объёмной (линейной) зоной обнаружения, требуется подготовить охраняемый участок (вырубить кусты, скосить траву, спланировать поверхность), руководствуясь рекомендациями эксплуатационной документации. Ширина зоны отторжения должна быть не менее указанной в эксплуатационной документации. В зоне отторжения не должно быть строений и предметов, затрудняющих применение технических средств охраны и действия сотрудников полиции.

Установка охранных извещателей по верху основного ограждения должна производиться при условии, что оно имеет высоту не менее 2,5 м. Максимальная дальность действия и высота установки извещателя от верхней части ограждения указываются в эксплуатационной документации.

Водопропуски сточных или проточных вод, подземные коллекторы (кабельные, канализационные) при диаметре трубы или коллектора 300 – 500 мм, выходящие с территории объекта, должны быть оборудованы металлическими решётками. Стальную решётку из прутка диаметром не менее 16 мм и ячейкой 50 х 150 мм приваривают к прочно заделанным в стену на глубину 80 мм стальным анкерам диаметром не менее 12 мм (к закладным деталям из стальной полосы 100 х 50 х 6 мм, пристреливаемым четырьмя дюбелями), с шагом не более 500 х 500 мм.

В трубе или коллекторе большего диаметра, где есть возможность применения инструмента взлома, необходимо устанавливать решётки, заблокированные ОС на разрушение и открывание.

На КПП, в помещении сотрудников полиции следует устанавливать технические устройства графического отображения охраняемого периметра (компьютер, световое табло с мнемосхемой охраняемого периметра и другие устройства).

Всё оборудование, входящее в систему СОС периметра, должно иметь защиту от вскрытия, металлические корпуса приборов должны быть заземлены.

Отдельные участки с материальными ценностями на территории объекта должны иметь предупредительное ограждение. Для защиты таких участков используются объёмные радиоволновые извещатели, предназначенные для блокировки открытых площадок или линейные оптико-электронные извещатели, предназначенные для блокировки периметра.

При наличии запретной зоны для прохода (проезда) в неё в ограждениях с интервалом не более 500 м оборудуются калитки (ворота). Их количество и место расположения выбираются исходя из условия максимального сокращения времени прибытия в запретную зону нарядов полиции, а также с учётом расположения КПП и других сооружений (зданий) по периметру объекта. Все калитки (ворота) должны быть оборудованы средствами постовой связи, ОС и замковыми устройствами.

При оборудовании периметра СОС необходимо учитывать наличие крыш и стен зданий, переходов трубопроводов и коммуникаций над и под заграждением, водостоки и др. В каждом таком случае может потребоваться свой, нетрадиционный подход к поставленной задаче и при необходимости организация дополнительного рубежа охраны.

Для исключения доступа посторонних лиц к извещателям, ППК, разветвительным коробкам, другой установленной на объекте ашаратуре охраны, должны приниматься меры по их маскировке и скрытой установке. Крышки клеммных колодок данных устройств должны быть опломбированы (опечатаны) электромонтёром охранно-пожарной сигнализации 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 ПЦН в составе ТС.

Примечания:

В случае отсутствия (с учётом объективных факторов) на объекте необходимых средств инженерно-технической укреплённости (забор, решётки на окнах и т.д.) либо оснащённости объекта средствами инженерно-технической укреплённости более низкого класса защиты, рекомендуется оборудовать объект дополнительными рубежами охраны с использованием средств охранной сигнализации и системы охранной телевизионной.

Организация дополнительных рубежей охраны должна быть согласована с подразделением охраны и руководством объекта.

3.4 Система тревожной сигнализации.

Для передачи тревожных извещений с объекта на пульт централизованной охраны (в центр оперативного управления, группу обеспечения служебной деятельности нарядов полиции) подразделения вневедомственной охраны о противоправных действиях в отношении сотрудников и работников органа, организации, подразделения системы МВД России (угроз террористического и криминального характера) объект должен оборудоваться устройствами тревожной сигнализации (ТС): механическими кнопками, радиокнопками, радиобрелоками, педалями и другими устройствами.

Устройства ТС на объекте должны устанавливаться:

- в специальных помещениях органа, организации, подразделения системы МВД России (помещения дежурных частей, комнаты хранения оружия, боеприпасов и специальных средств, для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, изоляторы временного содержания, архивы, хранилища, кассы и другие);
- у центрального входа в здание и запасных выходах из него;
- на всех наружных и внутренних постах охраны и в помещении охраны;
- в иных местах, регламентированных правовыми актами МВД России.

Ручные и ножные устройства ТС должны размещаться по возможности в незаметных местах.

3.5 Организация передачи информации о срабатывании сигнализации.

На ПЦН выводятся сигналы от ТС и об отключении основного электропитания системы охранной сигнализации.

3.6 Система передачи извещений (СПИ).

Система передачи извещений – совокупность совместно действующих технических средств, предназначенных для передачи по каналам связи и для приёма в пункт централизованной охраны извещений о состоянии охраны охраняемых объектов, служебных и контрольно-диагностических извещений, а также (при наличии обратного канала) для передачи и приёма команд телеуправления.

Рекомендуется применять объектовое оборудование СПИ, входящее в список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам

охраны, предназначенным для применения в подразделениях вневедомственной охраны».

Устройство оконечное объектовое (УОО) СПИ предназначено для организации централизованной охраны объектов в составе автоматизированной системы охранно-пожарной сигнализации. УОО осуществляет передачу на ПЦН извещений взят/снят, неисправность, проникновение. Выбор УОО целесообразно осуществлять с учётом применяемой СПИ, количества передаваемой информации, а также выбора каналов связи, обеспечивающего надёжность передачи информации.

Способ передачи информации с УОО на ПЦН зависит от типа СПИ, организации каналов связи и других факторов. Передача информации может осуществляться по занятой или выделенной телефонной линии, радиоканалу, каналу GSM (GPRS) или Ethernet, по GPON (оптоволокну) либо другому проводному каналу связи.

3.7 Прокладка проводов, кабелей.

Разводка шлейфов СОС по периметру территории выполняется в металлических коробах, металлических трубах или в металлорукаве проводами с медными жилами сечением не менее 0,4 мм. Соединение проводов должно осуществляться в герметичных металлических коробках соединительных.

3.8 Электропитание

Электропитание СОС осуществляется по 1 категории в соответствии с п. 9 Р 78.36.032-2013 и п. 1.2.17. ПУЭ издание 7 от свободной группы щитка дежурного освещения переменным током напряжением 220 В, 50 Гц.

При пропадании основного электропитания 220 В, 50 Гц СОС автоматически переходит на электропитание от резервного источника электропитания (аккумуляторов) постоянного напряжения 12 В (24 В) без выдачи сигналов тревоги, но с передачей соответствующего служебного сообщения (переход на электропитание от резервного источника).

При переходе на электропитание от резервного источника электропитания (аккумуляторов) должна обеспечиваться бесперебойная работа оборудования и извещателей СОС не менее 24 ч в дежурном режиме и не менее 3 ч в режиме тревоги.

Пример расчёта резервного источника электропитания 12 В (24 В) и аккумуляторов.

№	Наименование	Кол-во, шт.	Ток потребления одним устройством, мА	Суммарный ток потребления, мА
1	ППКОП	1	350	350

2	Извещатель охранный оптико-электронный линейный	8	90	720
3	Извещатель охранный радиоволновый линейный	8	70	560
	Итого			1630

Необходимая ёмкость аккумулятора рассчитывается по формуле:
Q(мАч) =1,2 х Iр (мА) х t (ч),
где:
Iр=1630 - потребляемый ток (мА);
t =24 - требуемое время работы (ч);
1,2 - коэффициент запаса ёмкости.
Необходимая ёмкость аккумулятора составляет:
1,2 х 1630 мА х 24 ч = 46944 мАч.

Таким образом, для электропитания ОС необходимо установить резервированный источник электропитания с выходным напряжением 12 В (24 В), током нагрузки не менее 1630 мА и подключаемых к нему аккумуляторных батарей ёмкостью не менее 46944 мАч.

ПРИЛОЖЕНИЯ

Схема блокировки калитки вибрационным и магнитоконтактным извещателем

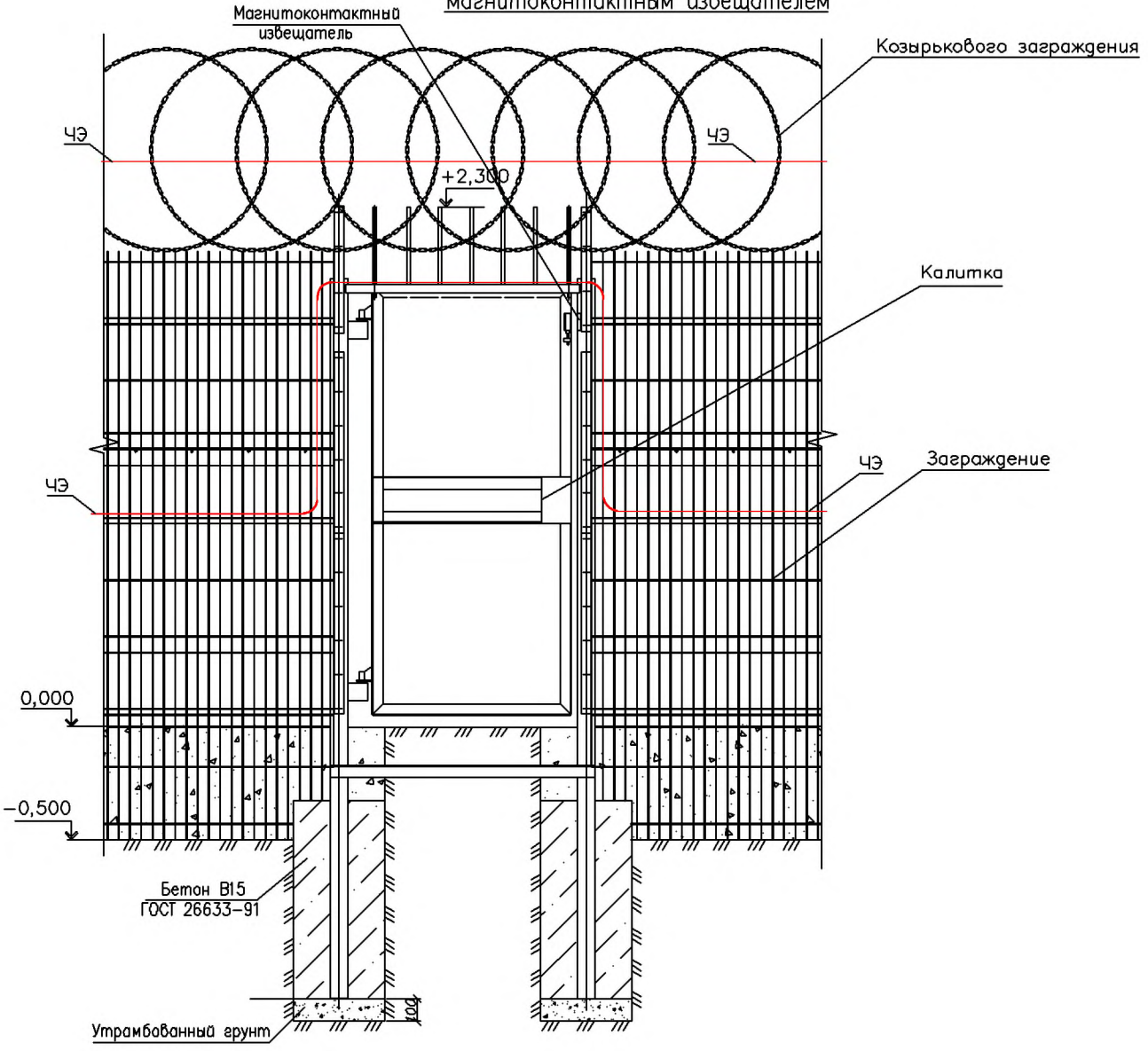
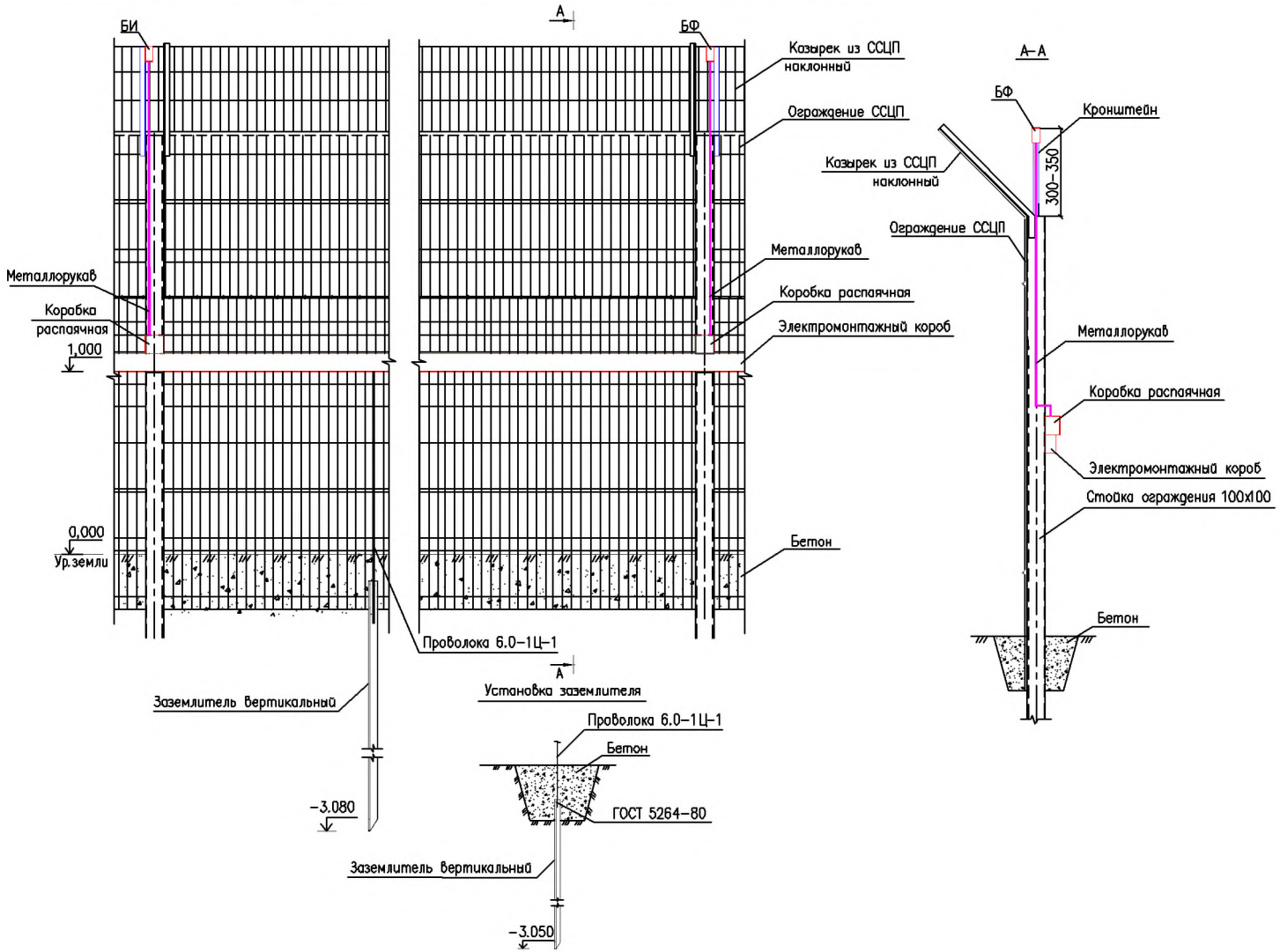


Схема блокировки ограждения от перелаза инфракрасным линейным извещателем



Пример защиты ограждения в два рубежа охраны
радиоволновым и инфракрасным линейными извещателями

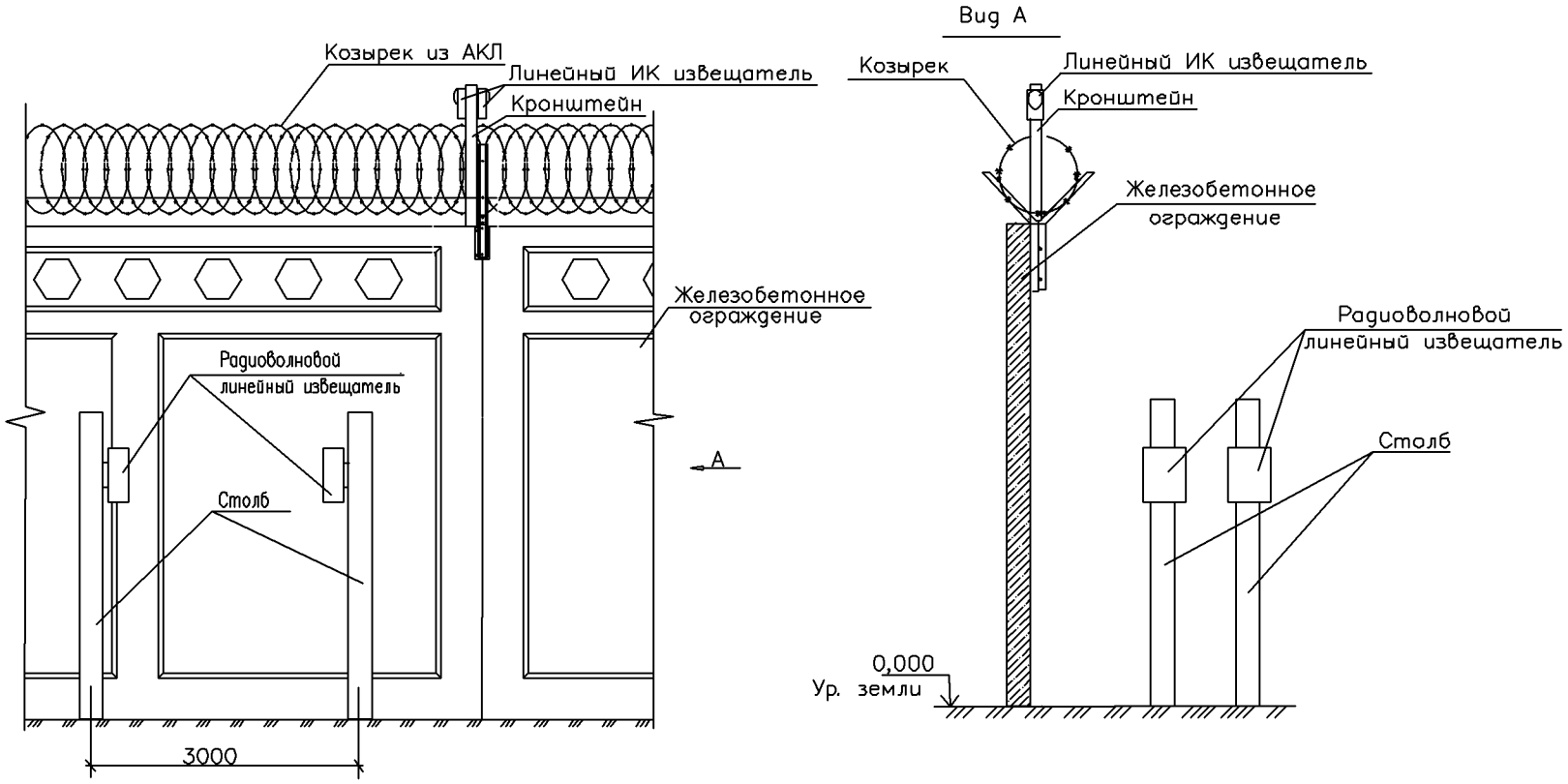
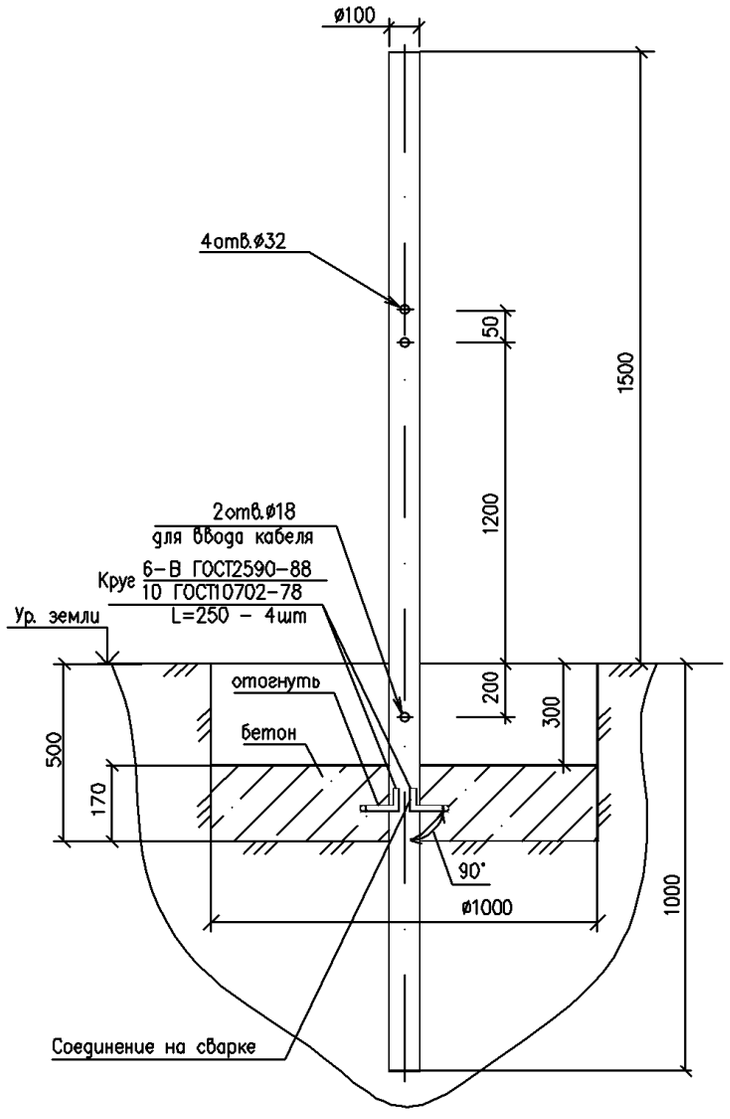
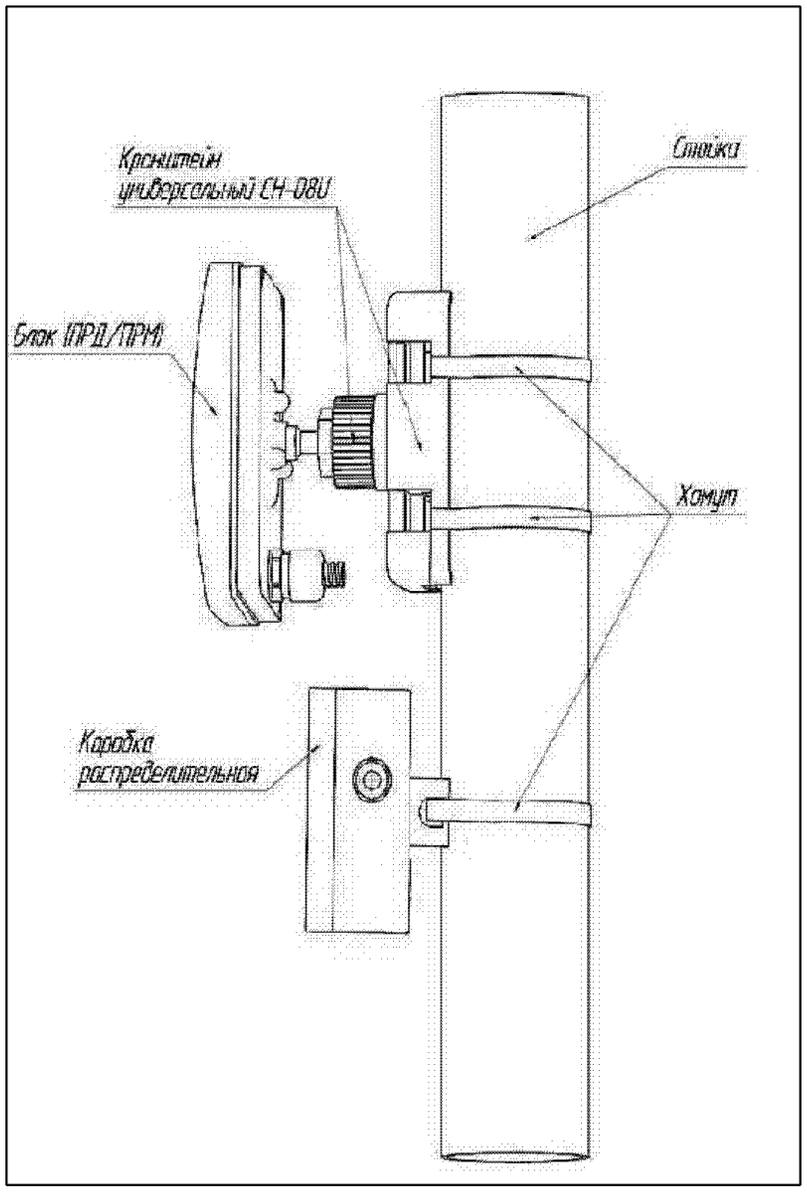


Схема монтажа извещателя охранного линейного радиоволнового





Варианты блокировки ограждения виброционным извещателем

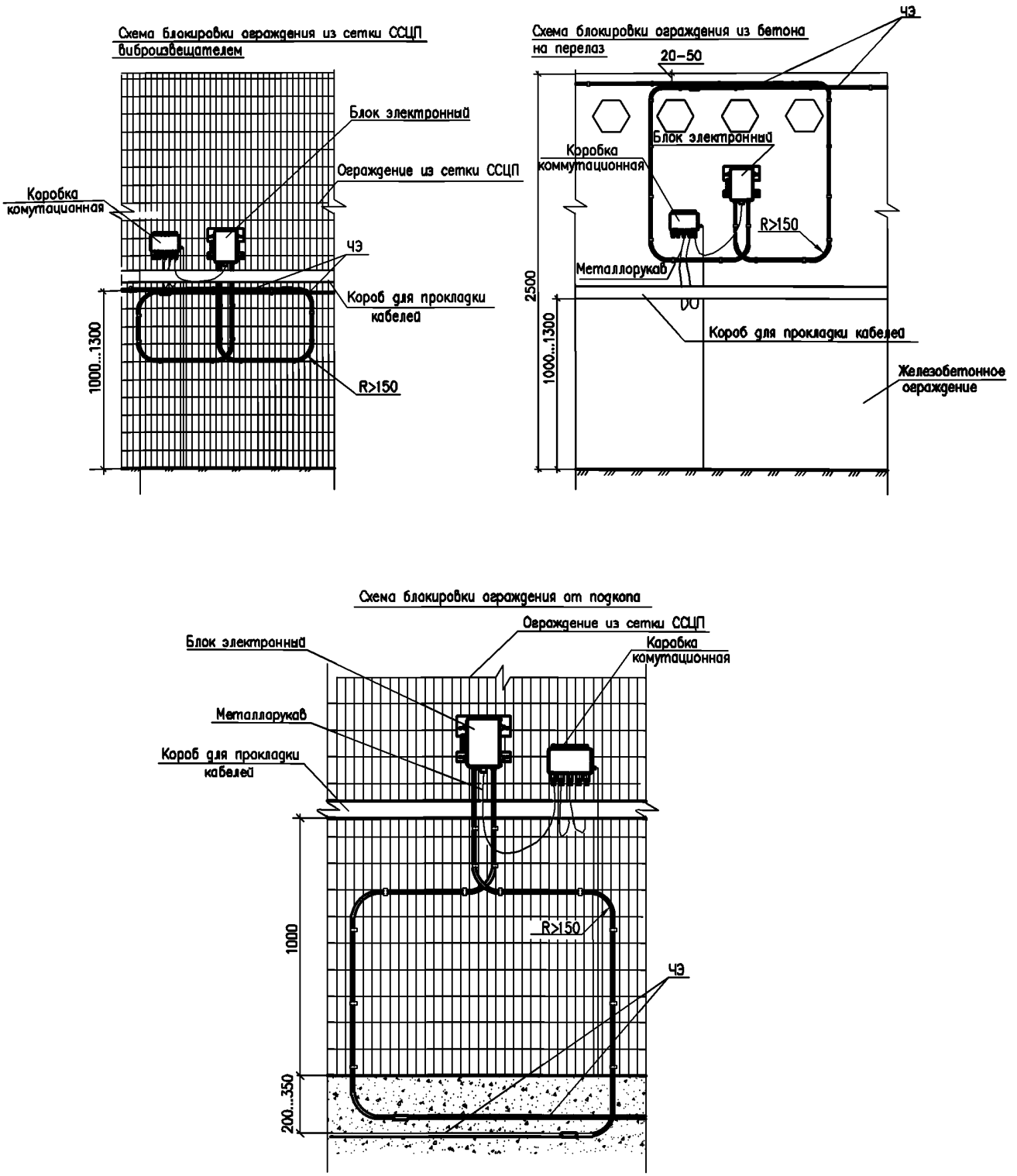


Схема блокировки ограждения емкостным извещателем

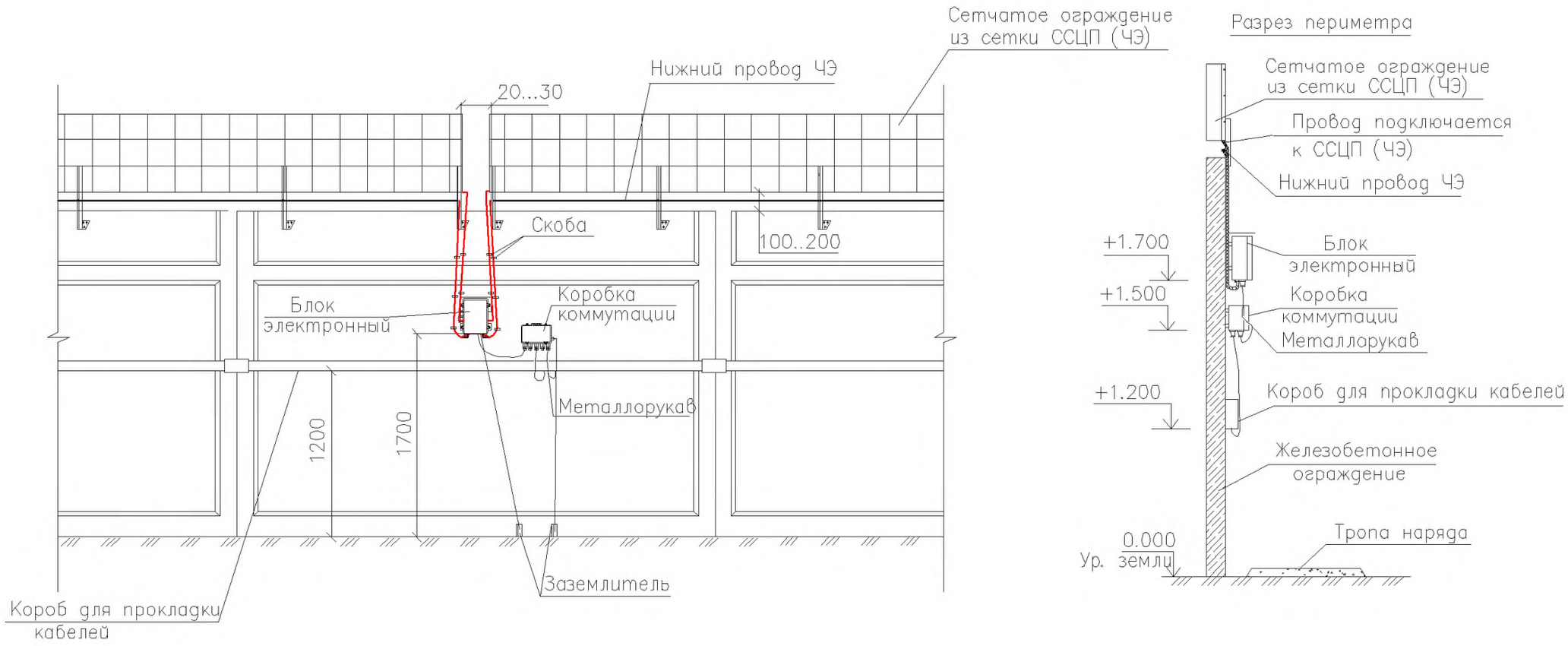
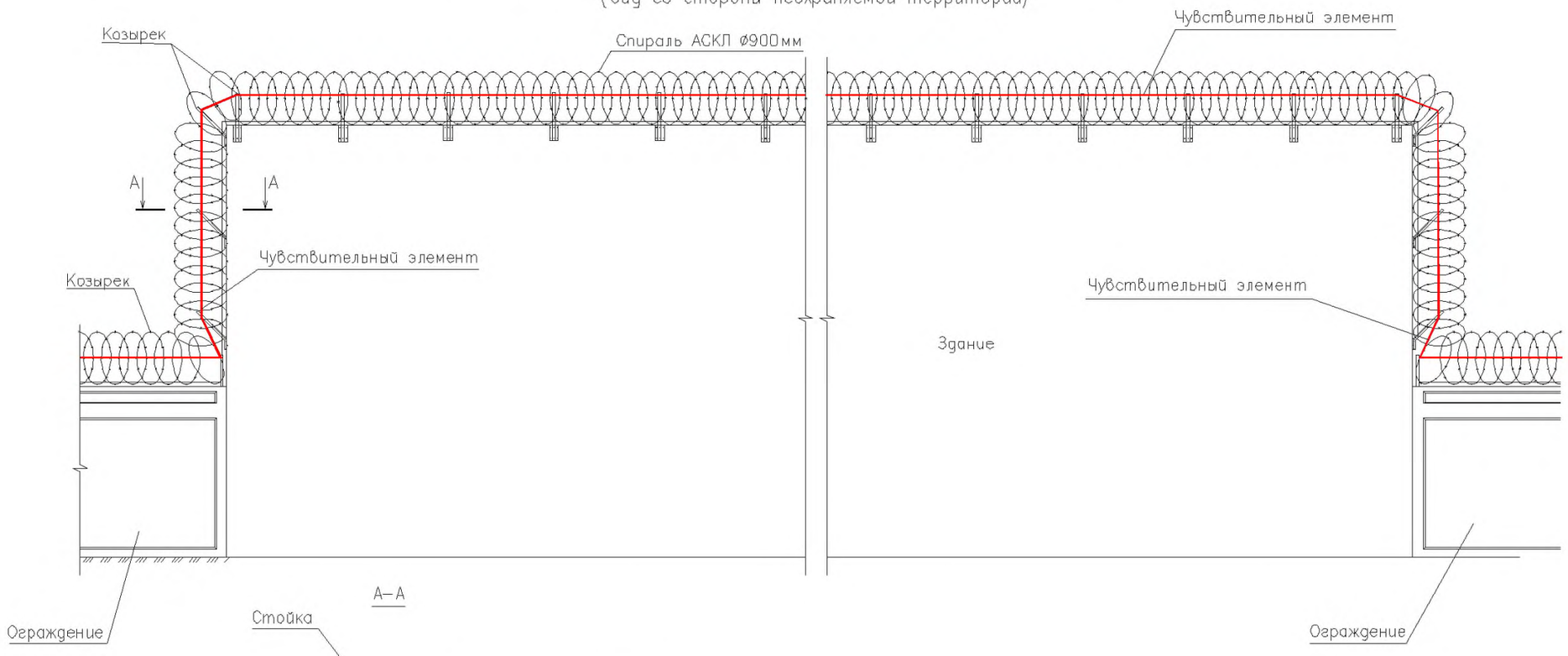


Схема блокировки от проникновения через здание вибрационным извещателем
(вид со стороны неохраняемой территории)



А–А

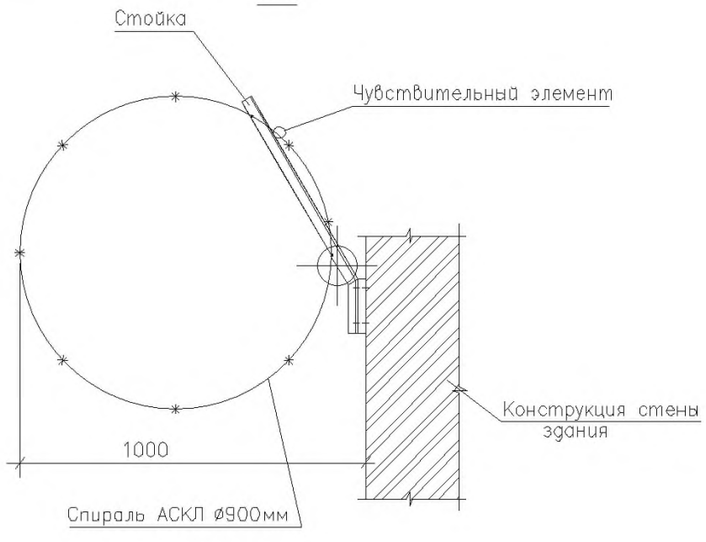


Схема блокировки ворот инфракрасным линейным извещателем от перелаза и на открывание магнитоконтактным извещателем

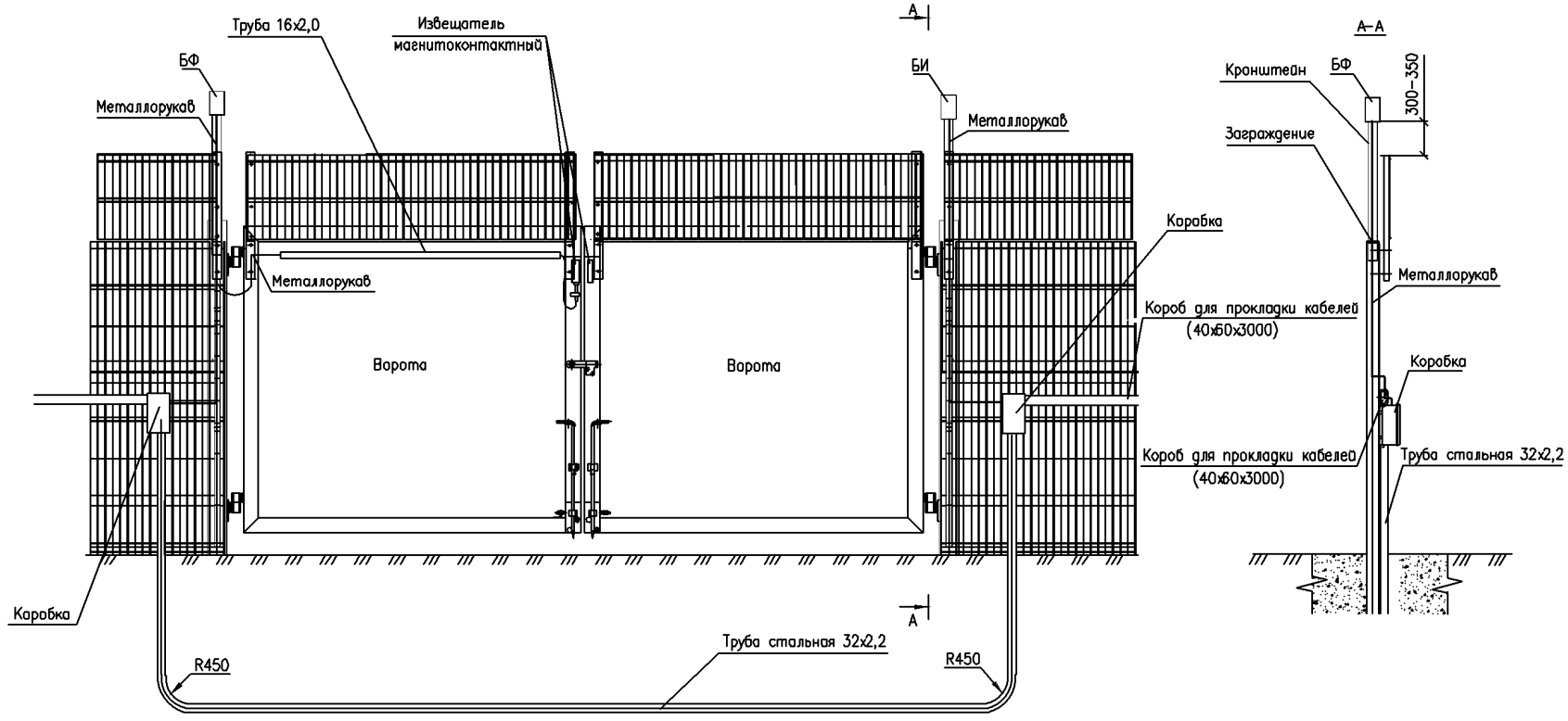
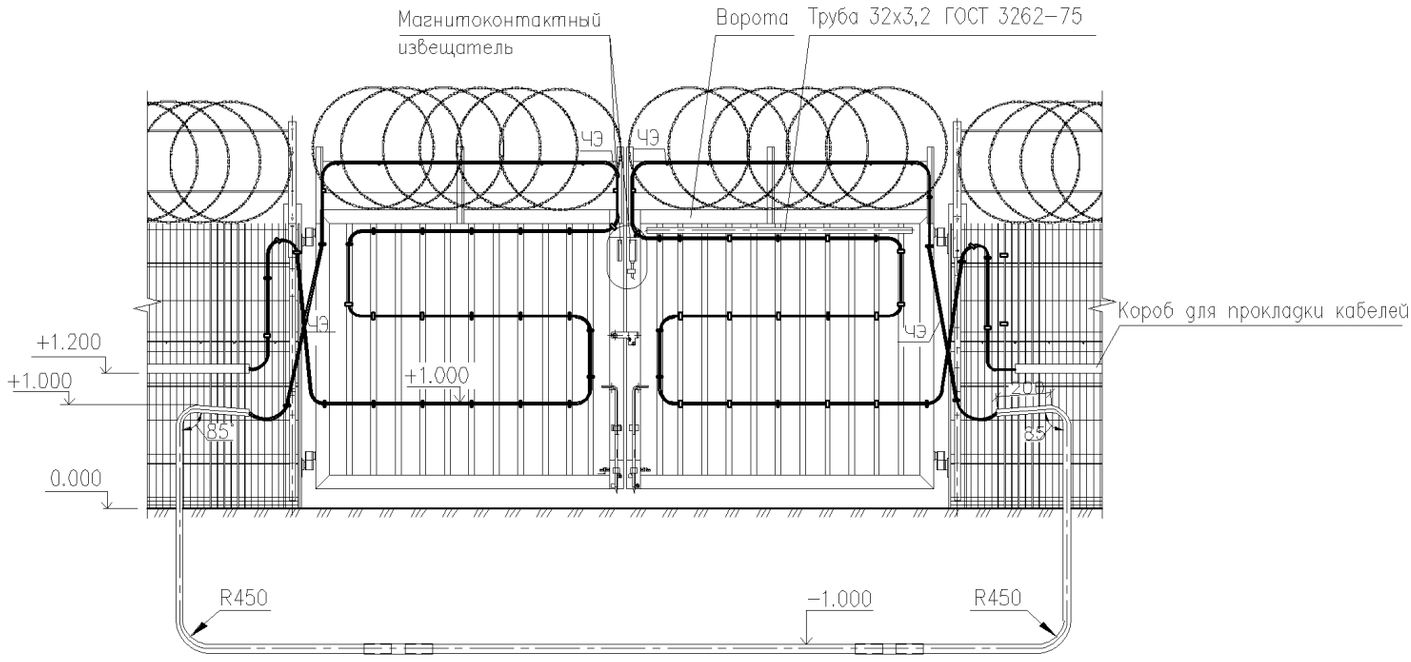
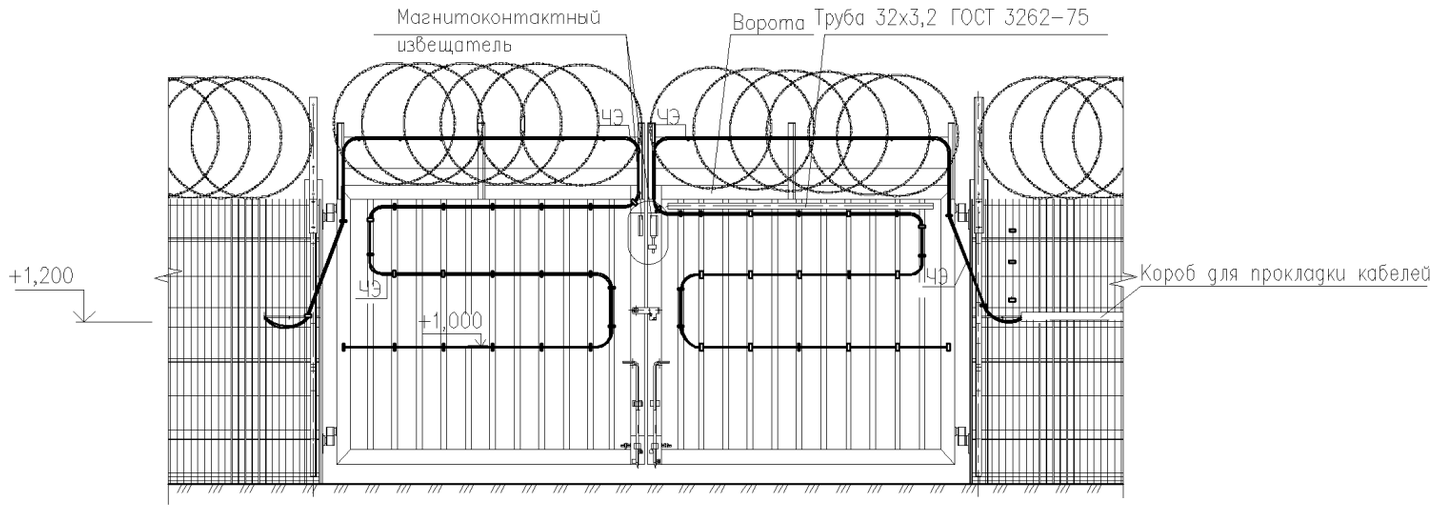


Схема блокировки ворот вибрационным и магнитоконтактным извещателями

Вариант 1

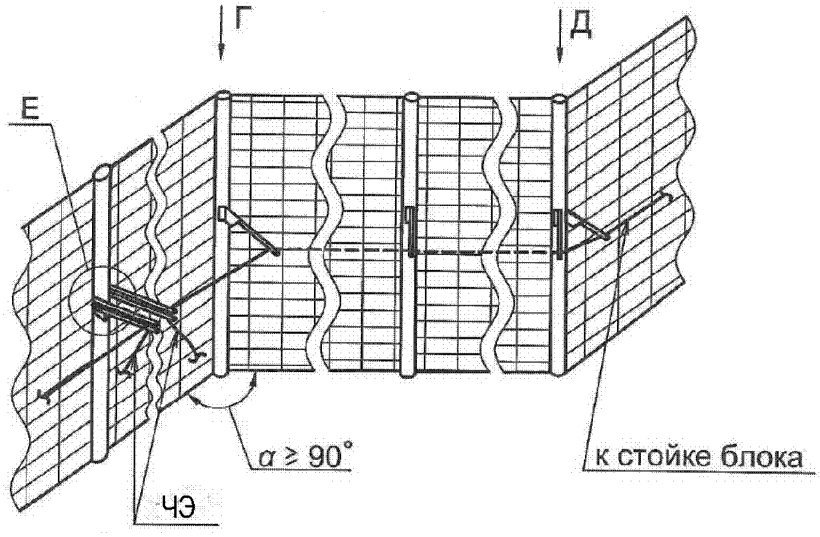


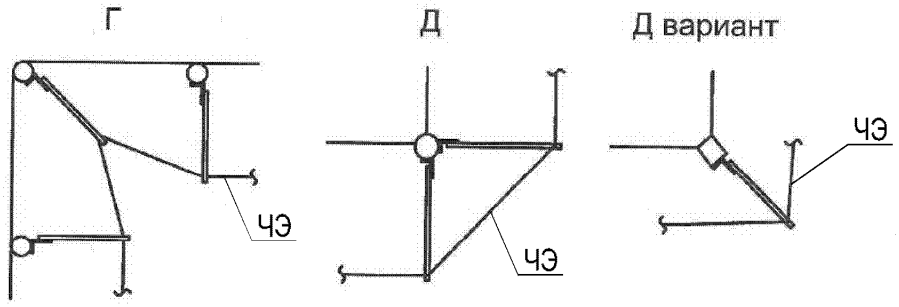
Вариант 2



Приложение 10

Схема блокировки сетчатого ограждения проводноволновым извещателем





Приложение 11

Схема блокировки на перелаз через здание проводноволновым извещателем

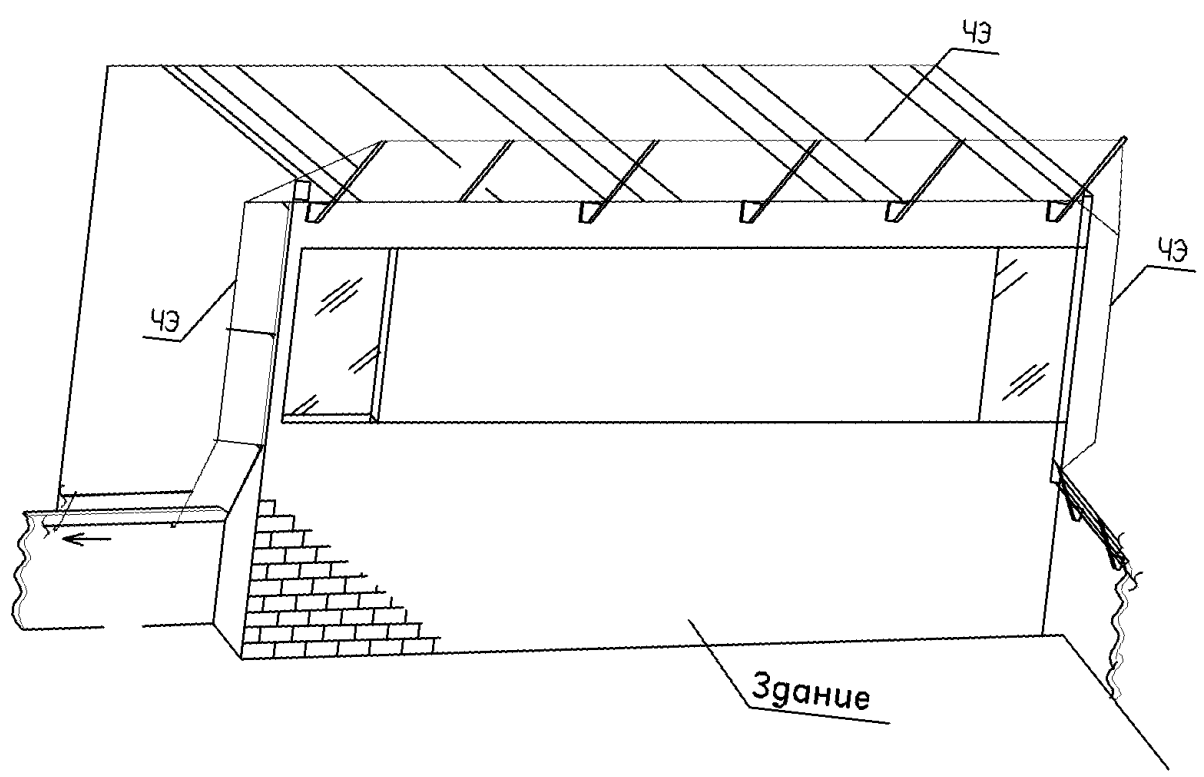
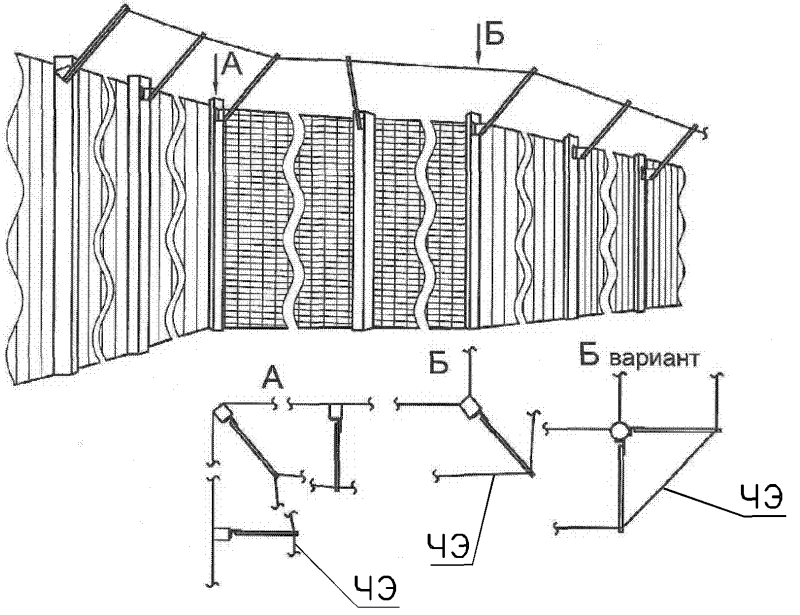


Схема блокировки сплошного ограждения от перелаза проводноволновым извещателем (вид1)



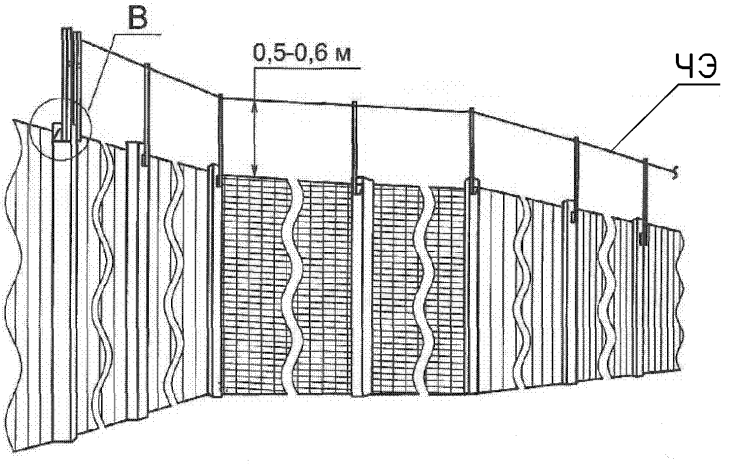


Схема блокировки сплошного ограждения от перелаза проводноволновым извещателем (вид 2)

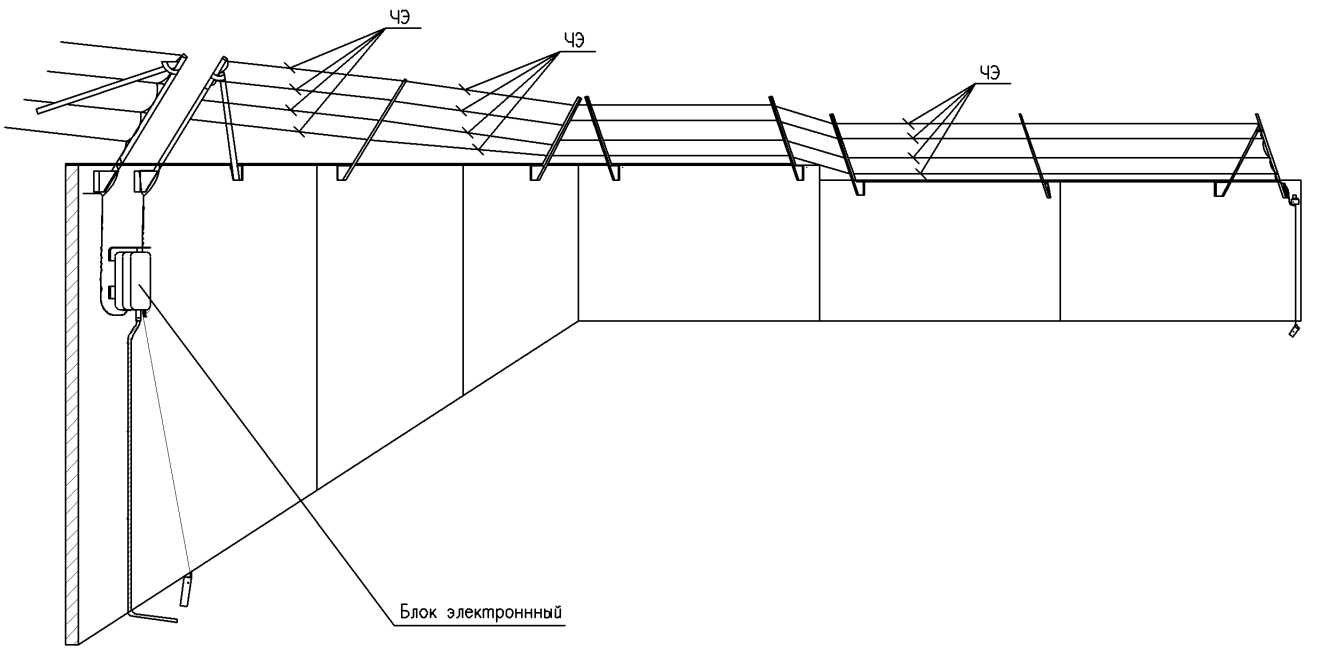


Схема блокировки ворот радиоволновым линейным и магнитоконтактным извещателем

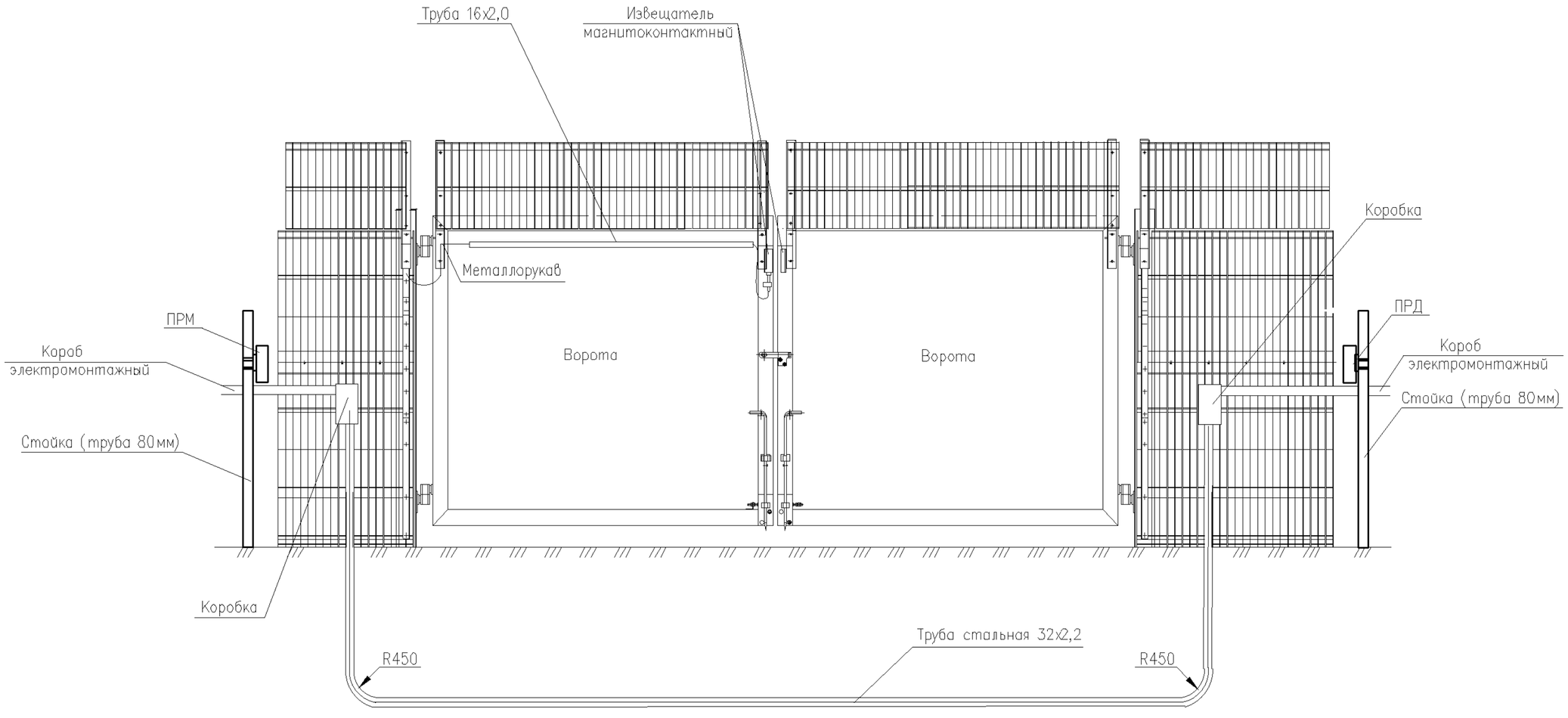
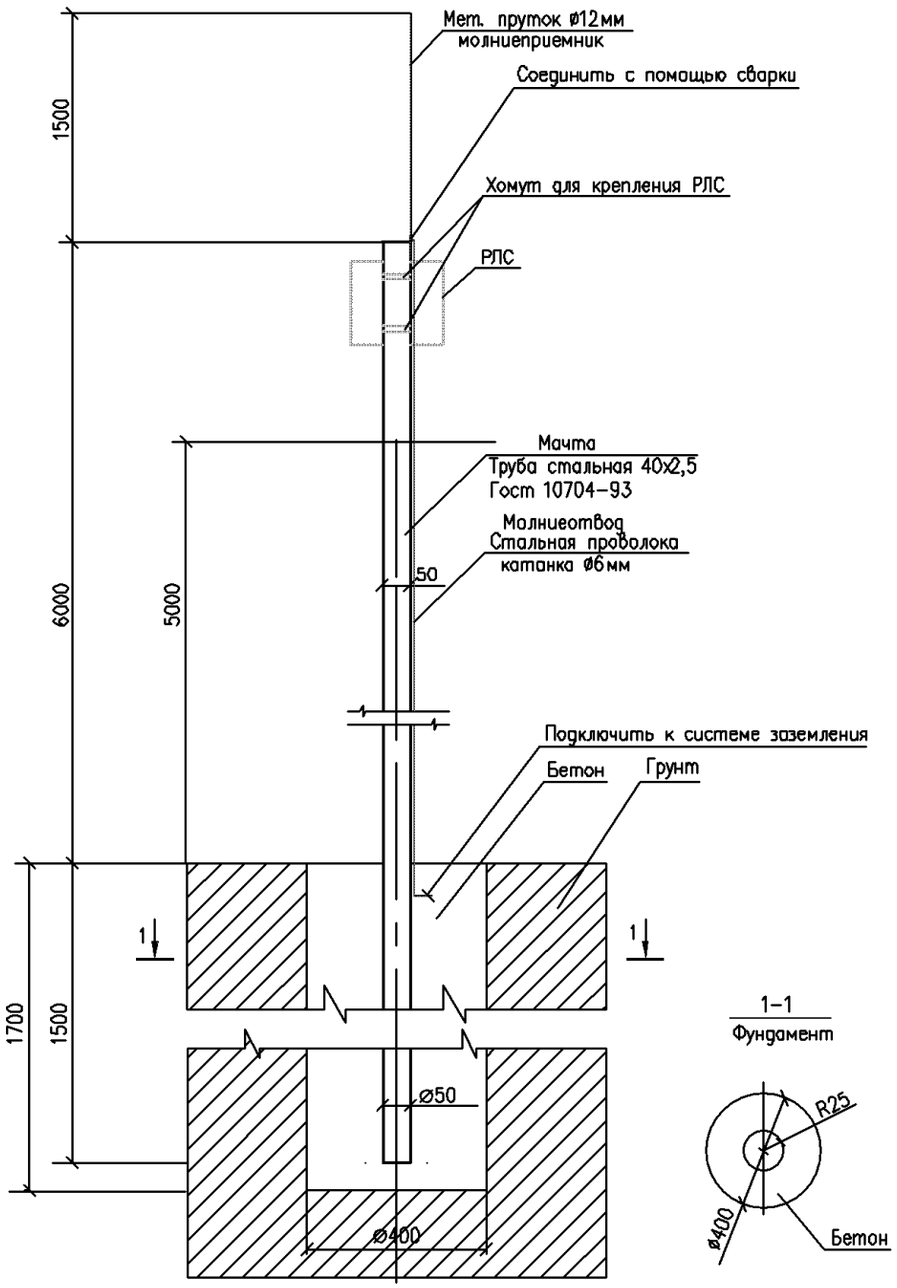
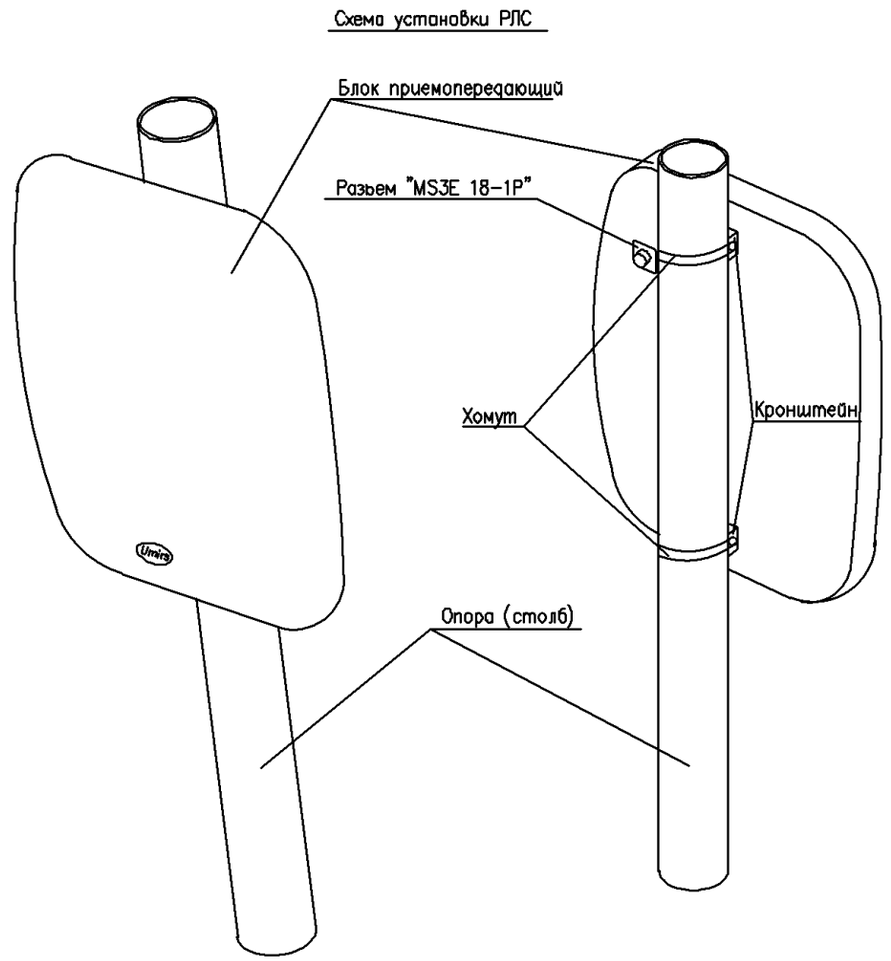
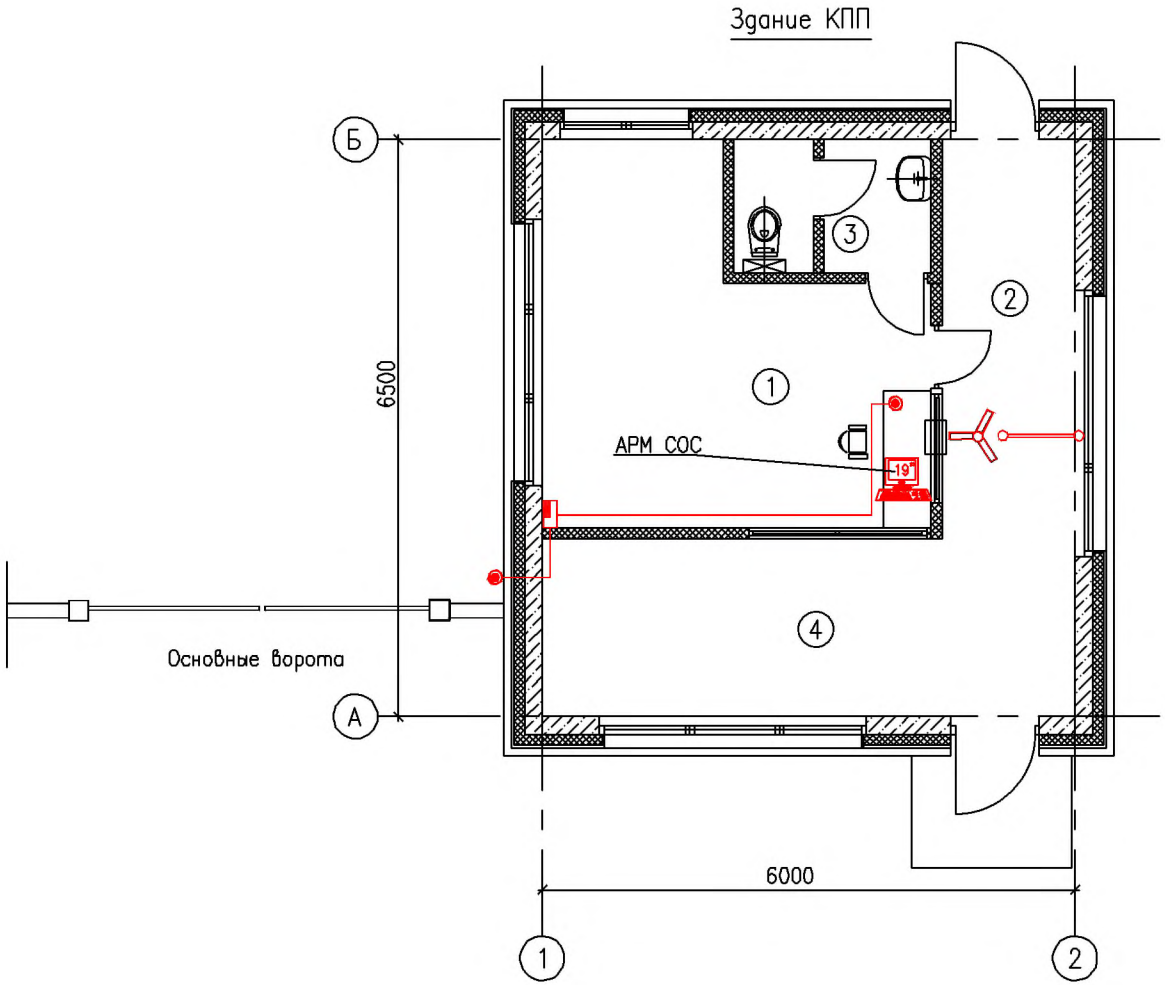


Схема установки радиолакационной станции с фиксированным углом обзора на столбе







Экспликация помещений

N п/п	Наименование	Площадь м²
1	Помещение охраны	
2	Коридор	
3	Санузел	
4	Холл	

Условные обозначения

Прибор приемно–контрольный охранно–пожарный

Кнопка тревожной сигнализации

Трасса прокладки кабеля

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к третьей категории»

Система охранная телевизионная

РАЗДЕЛ 3

Москва 2016 г

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	112
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	114
3.	СИСТЕМА ОХРАННАЯ ТЕЛЕВИЗИОННАЯ (СОТ)	115
3.1	Типы и виды СОТ. Их назначение и функции	115
3.2	Передача телевизионного сигнала	129
3.3	Расчёт объёма архива видеозаписи	130
3.4	Электропитание СОТ	131
3.5	Заземление	132
3.6	Критерии и принципы выбора СОТ	133
3.7	Общие требования к минимально необходимому составу СОТ	134

ПРИЛОЖЕНИЯ.

Приложение 1.	Условные обозначения.	137
Приложение 2.	СОТ периметра территории.	138
Приложение 3.	СОТ контрольно-пропускного пункта.	139
Приложение 4.	План расположения оборудования СОТ на 1-м этаже здания УВО.	140
Приложение 5.	План расположения оборудования СОТ на 2-м этаже здания УВО.	141
Приложение 6.	Структурная схема СОТ здания УВО.	142
Приложение 7.	Структурная схема СОТ периметра территории.	143
Приложение 8.	Схемы установки телевизионных камер на стене и потолке.	144
Приложение 9.	Схемы установки телевизионных камер на столбах.	145

ОБЩАЯ ЧАСТЬ

Методические рекомендации по оснащению ведомственных объектов СОТ разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 2.01.2013 № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;
- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;

- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 51558-2008 «Системы охранные телевизионные. Общие технические требования и методы испытаний»;
- ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- Р 78.36.005-2011 «Выбор и применение систем контроля и управления доступом»;
- Р 78.36.018–2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- Р 78.36.026-2012 «Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны ограждённых территорий и открытых площадок»;
- Р 78.36.027-2012 «Рекомендации по применению тепловизионного оборудования в системах охранного телевидения»;
- Р 78.36.028-2012 «Рекомендации. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов»;
- Р 78.36.029-2014 «Об оснащении ПЦО средствами аудио- и видеонаблюдения»;
- Р 78.36.030-2013 «Применение программных средств анализа видеоизображения в системах охранного телевидения в целях повышения антитеррористической защищённости ПЦО подразделений вневедомственной охраны»;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану. Методические рекомендации»;
- Р 78.36.032-2013 «Инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1. Объекты»;
- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения»;

- Р 78.36.042-2014 «Рекомендации по использованию комплекта оборудования для фиксации и передачи видеоинформации с охраняемого объекта на ПЦО»;
- Р 78.36.049-2015 «Применение оборудования охранных телевизионных систем в условиях ограниченной видимости или других дестабилизирующих факторов»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ - Правила устройства электроустановок (издание 7).

1. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

В соответствии с пунктом 4.3 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом III категории по степени потенциальной угрозы понимается отдельно стоящие здания или сооружения, имеющие прилегающую территорию (или без таковой), на которых осуществление круглосуточного пропускного режима и круглосуточного дежурства не обязательно.

3. СИСТЕМА ОХРАННАЯ ТЕЛЕВИЗИОННАЯ (СОТ).

3.1 Типы и виды СОТ. Их назначение и функции.

СОТ – телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений (со звуковым сопровождением или без него), служебной информации и извещений о тревоге с охраняемого объекта.

3.1.1 Типы и виды СОТ.

Аналоговая СОТ – система, в которой видеосигнал от видеокамер до видеомонитора и/или видеорегистратора передаётся в аналоговом виде, не подвергаясь аналого-цифровому преобразованию.

Цифровая СОТ – система, в которой видеосигнал от телевизионных камер (ТК) преобразуется в цифровую форму с помощью аналого-цифрового преобразователя и далее в СОТ обрабатывается в цифровом виде.

Комбинированная СОТ – система, содержащая элементы аналоговой и цифровой СОТ.

Основные общие элементы различных СОТ:

- ТК;
- тепловизор;
- устройства управления и коммутации видеосигналов;
- источник электропитания, в том числе резервного электропитания;
- соединительные линии;
- вспомогательное оборудование.

ТК делятся на:

- аналоговые и цифровые;
- корпусные и бескорпусные;
- для уличного и внутреннего применения;
- стационарные;
- поворотные;
- купольные;
- для применения в особых условиях;
- чёрно-белого и цветного изображения;
- повышенной чувствительности;
- высокого разрешения;
- вандалозащищённые;
- для скрытого наблюдения.

В зависимости от требований, предъявляемых к системе, ТК могут оснащаться различными устройствами: объективами, защитными или декоративными кожухами, термостатами, кронштейнами, поворотными устройствами и т.п.

ТК характеризуется набором параметров:

- формат матрицы;
- разрешающая способность (разрешение в центральной области изображения или объектива);
- чувствительность;
- синхронизация;
- электронный затвор;
- автоматическая регулировка диафрагмы (АРД);
- автоматическая регулировка усиления (АРУ);
- гамма-коррекция видеосигнала (коррекция);



Рисунок 1. ТК различного конструктивного исполнения.

- компенсация «засветки сзади» (компенсация засветки телекамеры при наблюдении за предметом, освещённым сзади ярким светом);
- канал звука;
- напряжение питания;
- автоматический баланс белого;
- стандарт кодирования цветового сигнала.



Рисунок 2. ТК в вандалозащищённом исполнении.



Рисунок 3. Внешний вид охранного извещателя с установленной внутри ТК.



Рисунок 4. Внешний вид пожарного извещателя с установленной внутри ТК.



Рисунок 5. ТК устанавливаемая на подвесном потолке.



Рисунок 6. Установка ТК с ИК-прожектором
на стене здания.



Рисунок 7. Установка ТК на столбе.



Рисунок 8. Поворотные роботизированные ТК.

3.1.2 Тепловизоры.

Применение тепловизионного оборудования в системах СОТ позволяет существенно повысить эффективность таких систем. Тепловизор менее зависим от ряда погодных условий, затрудняющих обнаружение (дождь, туман и т.п.), и позволяет наблюдать перемещение людей и автомобилей в таких условиях, когда обычная СОТ становится неэффективной.

Тепловизор позволяет обнаруживать цели типа «человек» на значительном удалении от рубежа охраны даже при использовании нарушителем маскировочного халата.

Возможности тепловизионного наблюдения в сложных погодных условиях значительно превосходят возможности телевизионного наблюдения.

Совместное применение тепловизоров и ТК является наиболее эффективным средством для обнаружения нарушителей.

Типы тепловизоров:

- стационарные;
- переносные;
- с охлаждением приёмника ИК-излучения;
- без охлаждения приёмника ИК-излучения.



Рисунок 9. Внешний вид стационарного тепловизора.

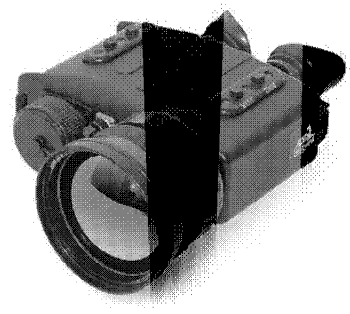


Рисунок 10. Внешний вид переносного тепловизора.

По типу структуры приёмника тепловизоры разделяются:

- в виде матрицы (например, 328x256 пиксела);
- в виде линейки (например, 288x4 пиксела).

По типу сканирования окружающего пространства:

- с механическим сканированием (при этом обычно применяется приёмник в виде линейки);
- без механического сканирования (при этом обычно применяется приёмник в виде одной или нескольких матриц).

Возможности тепловизора:

- работа в полной темноте;
- регистрация объекта при дожде и снеге.

Дальность регистрации объекта при дожде и снеге снижается незначительно, в тумане дальность регистрации объекта падает сильно, поэтому неправильно рассматривать тепловизор как абсолютное средство обнаружения.

Недостатки тепловизора:

Более низкое разрешение изображения, чем у прибора с зарядовой связью[1] (ПЗС-матрица) телевизионной камеры;

- высокая стоимость;
- тенденция к деградации матрицы, особенно для охлаждаемых матриц и сложных соединений типа КРТ[2]. Для болометра[3] на основе оксида ванадия время работы около 40000 часов (4,5 года).

Наиболее приемлемым типом тепловизора для использования является неохлаждаемый тепловизор на основе микроболометра.

---

[1] ПЗС — прибор с зарядовой связью. Общее обозначение класса полупроводниковых приборов, в которых применяется технология управляемого переноса заряда в объеме полупроводника. Название ПЗС — прибор с зарядовой связью — отражает способ считывания электрического потенциала методом сдвига заряда от элемента к элементу.

[2] КРТ - кадмий-ртуть-теллур.

[3] Болометр - прибор для измерения энергии электромагнитного излучения (главным образом инфракрасного), основанный на изменении электрического сопротивления термочувствительного элемента. в результате поглощения им энергии измеряемого излучения.





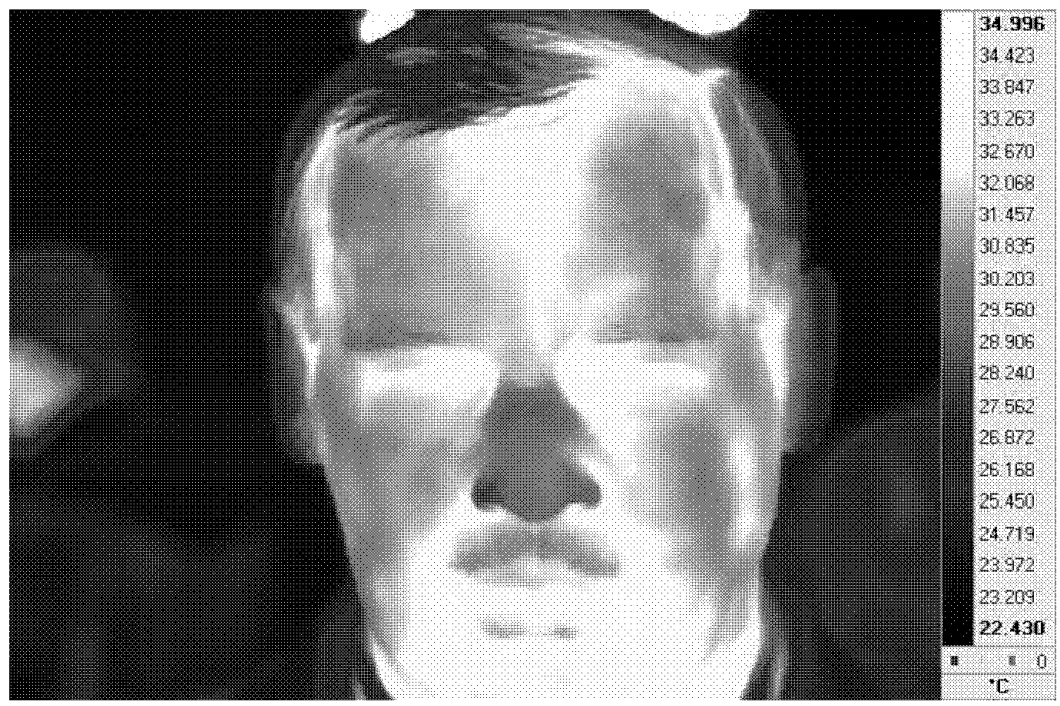


Рисунок 11. Примеры тепловизионных изображений.

3.1.3 Устройства обработки и коммутации видеосигналов.

Устройства обработки и коммутации видеосигналов – это устройства, управляющие потоками информации в СОТ: сигналами изображения, сигналами тревоги и управляющими сигналами. Использование устройств управления и коммутации видеосигналов позволяет существенно облегчить работу оператора, синхронизировать работу СОТ с другими системами безопасности объекта (системами охранно-тревожной сигнализации, контроля и управления доступом и др.).

Устройства обработки и коммутации видеосигналов подразделяются на:

- видеомониторы;
- видеокоммутаторы (Switcher);
- видеоквадраторы (Quadspliter);



Рисунок 12. Пример изображения, полученного тепловизором.



Рисунок 13. Пример изображения, полученного ТК.

- мультиплексоры (Multiplexer);
- матричные коммутаторы (Matrixswitcher);
- видеорегистраторы;
- выполненные на базе персональных и специализированных компьютеров.

3.1.4 Видеомониторы.

К параметрам, характеризующим монитор, относятся:

- диагональ экрана;
- соотношение сторон экрана;
- линейность;
- контрастность;
- яркость;
- строчная частота;
- кадровая частота;
- ширина полосы пропускания видеотракта.

Выбор монитора следует осуществлять таким образом, чтобы его разрешающая способность была выше, чем у применяемых ТК. Монитор не должен ухудшать общее разрешение системы.

3.1.4 Видеоквадраторы и видеокоммутаторы.

Видеоквадратор – это устройство, позволяющее одновременно выводить на экран видеомонитора изображения от четырёх источников видеосигнала, размещая их в соответствующих сегментах экрана.

Видеокоммутатор – это устройство, обеспечивающее последовательное переключение видеосигналов от нескольких ТК на один или несколько выходов (мониторов).

Видеокоммутаторы имеют автоматический и ручной режимы переключения ТК, позволяющие просматривать сигналы от всех ТК либо выборочно от некоторых из них.

Число входных видеоканалов может быть от 4 до 16, а при использовании нескольких блоков коммутации и более.

Видеоквадраторы и видеокоммутаторы для СОТ должны иметь дополнительные тревожные входы для подключения средств сигнализации. Количество дополнительных входов определяется количеством ТК.

Видеоквадраторы и видеокоммутаторы могут быть подключены к системе охранной сигнализации. При поступлении сигнала тревоги на видеоквадраторы и видеокоммутаторы от системы охранной сигнализации они должны выполнять следующие функции:

- вывод изображения в зоне тревоги на полный экран АРМ оператора;
- фиксацию изображения в одном из сегментов;
- передачу звукового сигнала тревоги;
- запись изображения тревожной зоны.

3.1.5 Видеомультиплексоры.

Видеомультиплексоры представляют собой системы видеозаписи и управления, обладающие широкими функциональными возможностями и предназначенные для записи видеосигналов от нескольких ТК на одно записывающие устройство (кодирование), воспроизведение кодированной информации и обработку сигналов тревоги.

Мультиплексоры позволяют осуществлять переключение между различными методами записи, что даёт возможность либо записывать изображение, появляющееся на экране, либо просматривать на экране изображения от одних ТК, записывая в это же время изображения от других ТК. Записанные изображения могут просматриваться на одном мониторе в полноэкранном режиме, режимах квадрированного экрана и "картинка в картинке" либо в мультиэкранном режиме, рисунок 10 (8+2, 9, 4+3, 12+1 или 16 сегментов на одном экране). Для более подробного анализа полноэкранных изображений многие мультиплексоры имеют функцию цифрового увеличения изображения: «ZOOM» (увеличение) позволяет увеличивать участок изображения относительно выбранной точки.



Рисунок 14. Изображение, выведенное на монитор в мультиэкранном режиме.



Рисунок 15. Рабочее место оператора СОТ.

Некоторые видеомультиплексоры имеют:

- возможность вывода изображения от любой подключённой ТК на любой из подключённых (как правило, до 4-х) мониторов;
- «телеметрические» функции (управление внешними устройствами);
- автоматическое и ручное «замораживание» кадра на экране дополнительного видеомонитора;
- контроль пропадания видеосигнала (пропадание входного видеосигнала видеомультиплексор воспринимает как «тревожную» ситуацию);
- цифровое увеличение изображения на экране дополнительного видеомонитора;
- балансировка яркости изображения от всех ТК (создание равно яркого квадрированного изображения);
- встроенные видеодетекторы движения;
- генераторы титров, даты и времени.



Рисунок 16. Образцы квадраторов и мультиплексоров.

3.1.6 Матричные видеокоммутаторы.

Матричный видеокоммутатор – это устройство, обеспечивающее соединение определённого числа ТК с определённым числом абонентов (мониторов, видеорегистраторов).

Главной задачей матричного коммутатора является переключение трансляции изображения (прямого или мультиплексированного) от любой ТК к любому абоненту системы по команде оператора или в автоматическом режиме.

Матричные коммутаторы по виду внутренней обработки видеоинформации делятся на аналоговые и цифровые.

3.1.7 Цифровые СОТ на базе персонального компьютера (ПК).

Типовая СОТ на базе ПК включает в свой состав одну или несколько плат видеозахвата и программное обеспечение (Рисунок 13).



Рисунок 17. Аналоговая система видеонаблюдения.



Рисунок 18. Один из вариантов комплектации СОТ на базе ПК.

3.1.8 СОТ на базе IP-видеонаблюдения.

В IP-видеонаблюдении используются в первом случае персональные компьютеры под управлением стандартной операционной системы (Windows и др.) с установленными специализированными платами «видеозахвата» и программным обеспечением для видеорегистрации, в другом случае цифровые видеорегистраторы являются специализированным оборудованием для IP-видеонаблюдения, устройствами, предназначенными под задачу видеорегистрации, то есть специально разработанное вычислительное устройство с максимально «облегченной» операционной системой (Linux, Windows, Embeded и др.), соответственно, максимально надёжное.

Цифровые гибридные видеорегистраторы позволяют осуществлять:

- видеорегистрацию цветного изображения с разрешением 700Твл;
- скорость регистрации на каждый канал 25 кадров/сек;
- общая скорость регистрации для 16 каналов составляет 400 кадров/сек;
- возможность использования одного из алгоритмов сжатия (M-JPEG, MPEG-2, MPEG-4, H.264).



Рисунок 19. Структурная схема СОТ с применением цифрового гибридного видеорегистратора.

Аналоговая передача сигнала по кабельным линиям подвержена ослаблению, искажению (необратимые потери) и имеет относительно невысокую помехозащищённость.

Для передачи изображения в IP-видеонаблюдении используется протокол TCP/IP и канал передачи информации Ethernet. IP-ТК передаёт видеоизображение в цифровом виде, используя алгоритм сжатия M-JPEG, MPEG-2, MPEG-4, H.264.

Каждое устройство, используемое в системе IP-видеонаблюдения (видеорегистратор, рабочая станция (компьютер) для просмотра видеоизображений), имеет персональный адрес.

В системе IP-видеонаблюдения информация имеет цифровой вид, что позволяет осуществлять её передачу и хранение без потерь.

В данных системах существует возможность использование ТК со сверхвысоким разрешением 1024x720 (720p), 1920x1080 (1080p, Full HD), 3МП (мегапиксела), 4МП, 8МП и т.д.

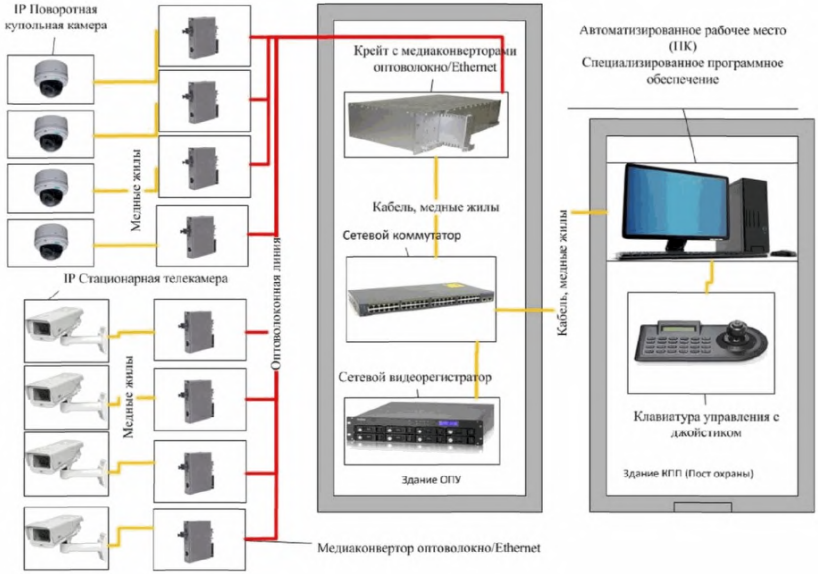


Рисунок 20. Структурная схема СОТ на базе IP-видеонаблюдения.

В системах IP-видеонаблюдения имеются следующие возможности:

- дистанционное конфигурирование параметров IP-ТК;
- тиражирование видеопотоков большому количеству конечных потребителей – «multicasting», что минимизирует трафик в сети и снижает требования к аппаратной части серверов и рабочих станций (компьютеров);
- резервирование магистральных линий связи, что обеспечивает дублирование линий связи между активными коммутационными устройствами (сетевыми коммутаторами, видеорегистраторами и прочими);
- видеонаблюдение и передача видеоинформации (видеопотоков) на большие расстояния через ИСОД (ЕИТКС) МВД России или интернет;
- использование функции Powerover Ethernet (PoE) – электропитание IP-ТК по тому же кабелю («витая пара»), по которому происходит передача видеоданных, что исключает необходимость в прокладке

отдельного кабеля питания к каждой телекамере и в случае большой распределенной системы является очень эффективным. (Использование этой возможности предполагает установку сетевого коммутатора с функцией PoE);

– видеорегистрация на iSCSI RAID[4]-массивах, которые подключаются непосредственно к активным коммутационным устройствам – сетевым коммутаторам.

3.1.9 Устройства регистрации.

Реализация цифровых устройств видеорегистрации осуществляется с помощью специализированных видеорегистраторов (DVR) и СОТ на базе ПК.

Преимущества DVR:

– высокая надежность;
– простота в управлении;
– небольшие размеры.

Гибридные DVR – аппараты, способные записывать сигналы одновременно с аналоговых ТК и IP-ТК, при этом не происходит потери качества изображения.

3.2 Передача телевизионного сигнала.

Для передачи телевизионного сигнала в СОТ могут использоваться как проводные каналы связи (коаксиальные кабели, симметричные проводные линии типа «витая пара», телефонные линии, волоконно-оптические линии), так и беспроводные каналы (радиоканал или ИК-канал).

Наиболее стабильная и качественная работа системы обеспечивается при использовании волоконно-оптических линий и коаксиальных кабелей.

Основными характеристиками коаксиального кабеля являются его волновое сопротивление, диаметр (как правило, чем больше диаметр кабеля, тем меньше затухание сигнала в нем) и погонное затухание, эффективность экранирования, степень защиты внешней оболочки (одной из важнейших характеристик является огнестойкость), климатическое исполнение.

Входные и выходные сопротивления основных компонентов СОТ имеют значение 75 Ом, применение кабелей с волновым сопротивлением 75 Ом не допускается.

Использование для передачи видеосигнала оптоволокна полностью исключает наводки на него.

Для передачи сигнала по кабелю «Витая пара» необходимо использование специального оборудования (приёмник и передатчик сигнала).

Преимущества передачи сигнала по «витой паре»:

---

[4]RAID — массив из нескольких дисков, управляемых контроллером, связанных между собой скоростными каналами передачи данных и воспринимаемых внешней системой как единое целое. В зависимости от типа используемого массива может обеспечивать различные степени отказоустойчивости и быстродействия.

- помехозащищённость линий передачи от низкочастотных помех (в первую очередь от сетевой наводки в 50 Гц);
- увеличение длины линии трансляции: для цветного видеосигнала составляет до 1000 м, для черно-белого – до 2000 м.



Рисунок 21. Передатчик видеосигнала по витой паре.



Рисунок 22. Приемник видеосигнала по витой паре.

Недостатки кабеля типа «витая пара»:

- искажение исходного видеосигнала по сравнению с коаксиальным кабелем;
- использование видеоусилителей и модемов (передатчики-модуляторы и приёмники-демодуляторы) для передачи сигнала на большие расстояния;
- использование на линиях передачи видеосигнала устройств грозозащиты.

3.3 Расчёт объёма архива видеозаписи.

На размер объёма архива видеозаписи существенно влияет ряд факторов:

- индивидуальная настройка для каждой ТК;

- осуществление цифровой мультиплексной записи одновременно по всем ТК;
- программирование приоритета при записи тревожных событий;
- программирование времени и скорости записи предтревожной ситуации;
- программирование режимов записи в зависимости от приходящих внешних сигналов тревоги и наличия движения в кадре.

Запись событий может включаться по сигналу тревоги на заданное время, сохранять одиночный кадр или вестись непрерывно.

Расчёт архива хранения сводится к определению размера кадра изображения, темпа записи кадров в секунду на каждую ТК, необходимого интервала времени для записи. Все эти данные определяются по согласованию с Заказчиком.

Пример расчёта объема архива записи при записи в режиме реального времени.

Разрешение ТК	Темп записи, кадр/сек	Размер кадра, кБ	Объём архива на камеру за день, ГБ	Количество записываемых ТК	Архив, дней	Общий объём архива, ТБ
704x576	25	13	28,08	16	30	13,48

Применяемые жёсткие диски в устройствах архивирования видеозаписей должны обеспечивать непрерывную работу не менее, чем 3 года, при условии круглосуточной видеозаписи информации от всех ТК.

3.4 Электропитание СОТ.

Электропитание СОТ осуществляется по 1 категории от отдельной группы щита дежурного освещения переменным током напряжением 220 В, 50 Гц.

При пропадании основного электропитания СОТ должна автоматически переходить на электропитание от резервного источника электропитания.

Согласно требованию п. 5.9.8. ГОСТ Р 51558-2014 при переходе на электропитание от резервного источника электропитания должна обеспечиваться бесперебойная работа системы не менее 0,5 часа.

Пример расчёта бесперебойного источника питания напряжением 220 В, 50 Гц.

	Наименование	Кол-во, шт.	Потребляемая мощность, ВА	Суммарная потребляемая мощность, ВА
1	Монитор 22”	1	250	250
2	Цифровой видеорегистратор	1	250	250
3	Коммутатор	1	40	40
4	Источник питания для ТК	1	200	200
5	ИТОГО			740

Q(Ач) = Pp/U x t(ч)x1,2,

где:

Pp - потребляемая мощность СОТ 740 ВА;

U- выходное напряжение аккумуляторов 12 В;

t - требуемое время работы 0,5 ч;

1,2 - коэффициент запаса ёмкости.

Необходимая ёмкость источника электропитания напряжением 220 В составляет:

740 ВА/12 В x 1,2 x 0,5 ч = 37 Ач.

Согласно расчётам, выбирается бесперебойный источник электропитания напряжением 220 В, 50 Гц, удовлетворяющий следующим характеристикам:

– минимальная нагрузка источника не менее 740 ВА;

– ёмкость аккумуляторных батарей должна быть не менее 37 Ач.

Электропитание всех элементов СОТ необходимо осуществлять от одной и той же фазы силовой сети.

3.5 Заземление.

Технические решения, использованные при заземлении, во многом определяют качество работы СОТ. При организации заземления необходимо руководствоваться следующими принципами:

Аппаратура СОТ должна быть заземлена, зануление аппаратуры СОТ недопустимо.

Приборы гальванической развязки включаются в разрыв кабельной линии связи, разрывая паразитный контур заземления.

Заземление оборудования и устройств должно выполняться в соответствии с требованиями СНиП 3.05.06-85, ПУЭ, технической документации предприятий-изготовителей.

3.6 Критерии и принципы выбора СОТ.

Выбор системы следует производить с учётом необходимой информативности СОТ, характеристик охраняемого объекта (расположение на местности, освещённость и другие признаки) и возможных объектов наблюдения (человек, автомобиль и другие цели).

Следует предусмотреть использование ТК, монтируемых в герметичных термокожухах, имеющих солнцезащитный козырёк и ориентированных на местности под углом к линии горизонта во избежание попадания лучей восходящего и заходящего солнца в объектив ТК.

Высота установки и тип крепления ТК должны исключать возможность их умышленного повреждения.

Для организации наблюдения территории в тёмное время суток необходимо предусмотреть систему охранного электроосвещения с учётом системы электроосвещения объекта и применения ТК с инфракрасной подсветкой.

Для наблюдения ТК протяжённых участков территорий объекта в проекте следует предусмотреть совместно с ТК объективы с переменным фокусным расстоянием и/или поворотные устройства и трансфокаторы с дистанционным управлением.

Уличные ТК должны комплектоваться объективами с автоматической регулировкой диафрагмы.

Для отображения поступающей с ТК информации необходимо предусмотреть применение специальных мониторов, работающих круглосуточно в течение длительного времени с неподвижным изображением.

ТК должны быть установлены так, чтобы исключить образование мёртвых зон, не контролируемых ТК.

Для записи телевизионных изображений следует предусмотреть применение цифровых видеорегистраторов.

Система охранная телевизионная с цифровым видеонакопителем должна аппаратно обеспечивать получение кадра на выходе системы не менее 720 х 576 пикселей.

Конструктивно СОТ должна строиться по модульному принципу и обеспечивать:

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

Для повышения вероятности обнаружения попыток проникновения следует использовать программные модули видеоаналитики.

3.7 Общие требования к минимально необходимому составу СОТ.

3.7.1 Минимально необходимый состав СОТ.

Объекты органов внутренних дел Российской Федерации, отнесённые к III категории, должны быть оборудованы СОТ.

Видеонаблюдение должно осуществляться:

- за периметром территории объекта и КПП (Приложения 2, 3);
- за периметром зданий и сооружений объекта, их входов и въездов-выездов (Приложение 4);
- за специальными помещениями и подходами к ним (Приложение 4, 5).

ТК устанавливаются на КПП (Приложение 3):

- для видеонаблюдения за входной дверью со стороны внешней территории;
- для видеонаблюдения за входной дверью со стороны внутренней территории;
- для видеонаблюдения внутри пропускного коридора;
- для видеонаблюдения за действиями сотрудника, несущего службу на КПП.

В помещении дежурного по контрольно-пропускному пункту и в дежурной части устанавливаются мониторы.

3.7.2 Функции СОТ.

СОТ должна выполнять следующие функции:

- оперативный доступ к видеозаписи и видеоархиву путём установления времени, даты и идентификатора телевизионной камеры;
- разграничение полномочий доступа к управлению системой в целях предотвращения несанкционированных действий;
- активирование телевизионных камер по сигналам охранной сигнализации или видеодетекторов движения;
- отображение видеоинформации в режиме реального времени;
- запись видеоинформации в режиме 25 кадров в секунду по каждому каналу (с каждой ТК) при максимальном качестве видеоданных;
- просмотр видеоархива любой телевизионной камеры без остановки записи;
- хранение видеоинформации в течение не менее 30 суток;
- приём видеоинформации, передаваемой по сети «Ethernet», одновременно с сообщениями, командами управления и речевыми переговорами;
- включение в локальную сеть нескольких автоматизированных рабочих мест;

- видеонаблюдение;
- видеонаблюдение в ночное время;
- подключение уличных купольных (управляемых) полноприводных цветных ТК с переключением режимов день/ночь;
- вывод видеоинформации от любой ТК на любое автоматизированное рабочее место по команде оператора или по событию в системе охранно-тревожной сигнализации и системе контроля и управления доступом (тревожной ситуации).

Примечания:

1. Аттестованные помещения, а также помещения, предназначенные для обработки сведений, составляющих государственную тайну, оборудуются техническими средствами, прошедшими сертификацию по стандартам ФСТЭК России и ФСБ России.

2. В случае отсутствия (с учетом объективных факторов) на объекте необходимых средств инженерно-технической укреплённости (решётки на окнах и т.д.) либо оснащённости объекта средствами инженерно-технической укреплённости более низкого класса защиты, рекомендуется оборудовать объект дополнительными рубежами охраны с использованием средств охранной сигнализации и СОТ.

Организация дополнительных рубежей охраны должна быть согласована с подразделением охраны и руководством объекта.

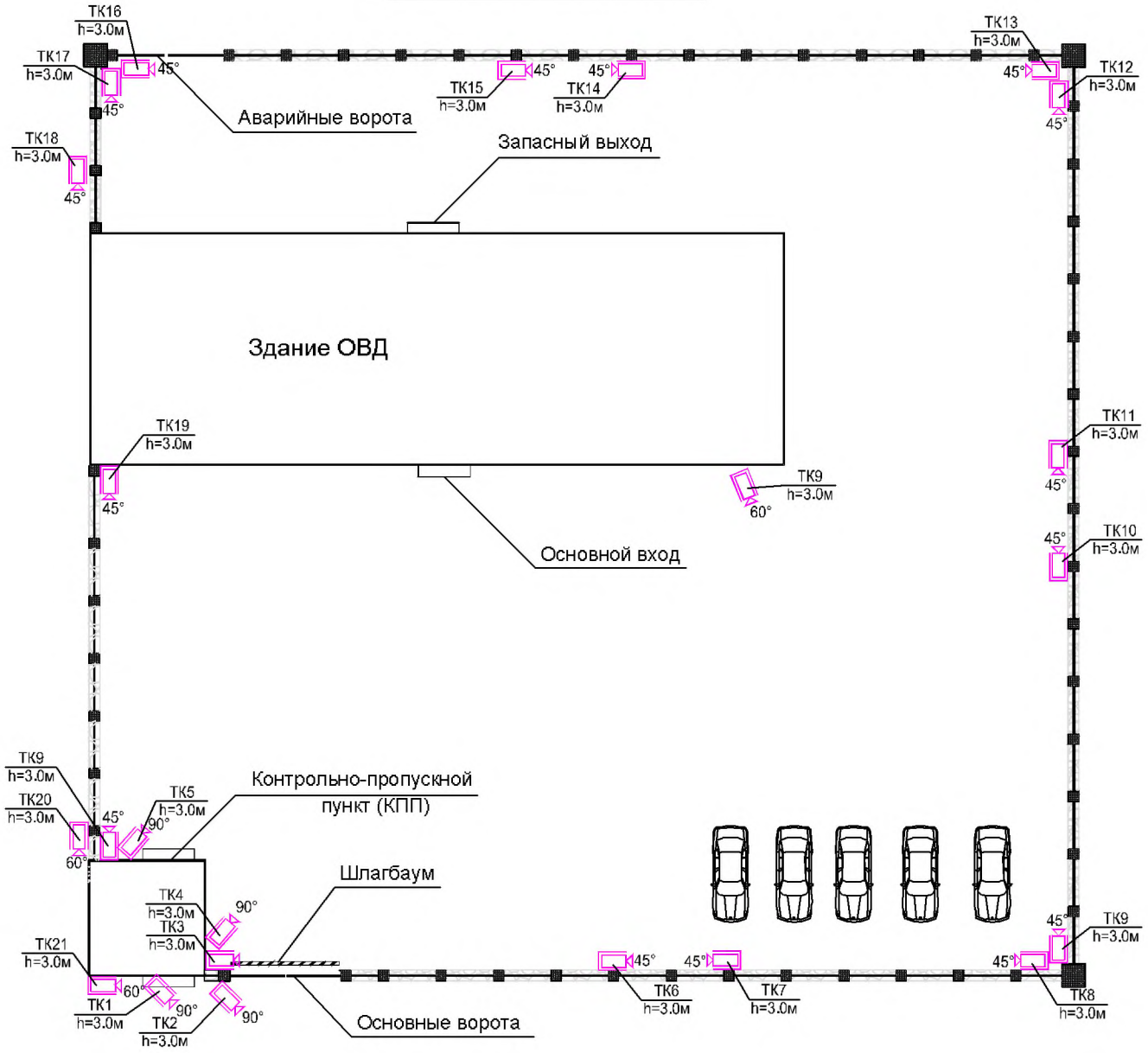
ПРИЛОЖЕНИЯ

Приложение 1

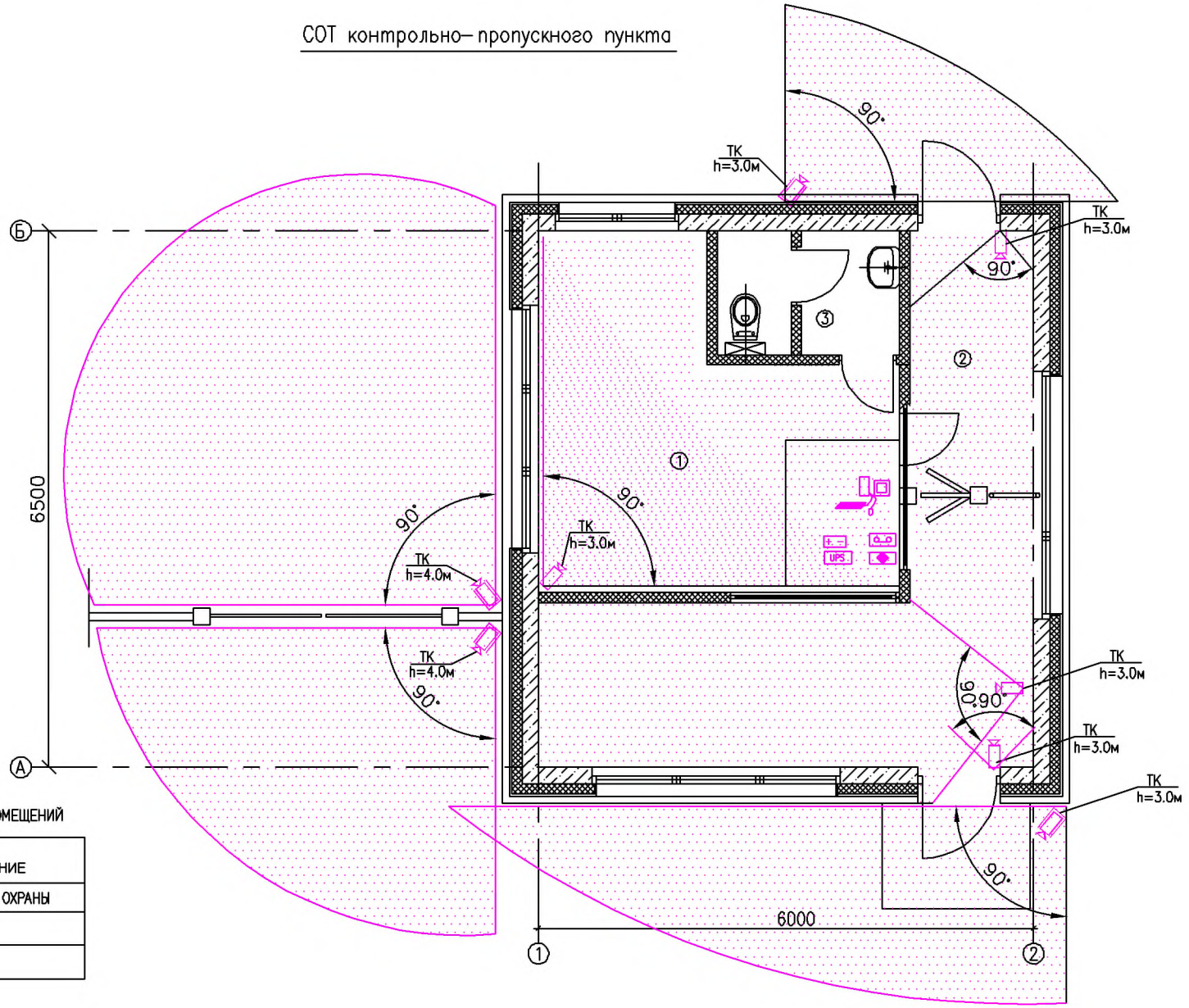
Условные обозначения

Наименование	Обозначение	
	на планах	на схемах
Видеомонитор		
Видеокамера, установленная в термокожухе, с обозначением угла обзора		
Видеокамера с обозначением угла обзора Видеокамера с обозначением угла обзора		
Коммутатор		
Видеорегистратор		
Источник питания 12В для видеокамер		
Источник бесперебойного питания, 220В,50Гц		

СОТ периметра территории



СОТ контрольно–пропускного пункта

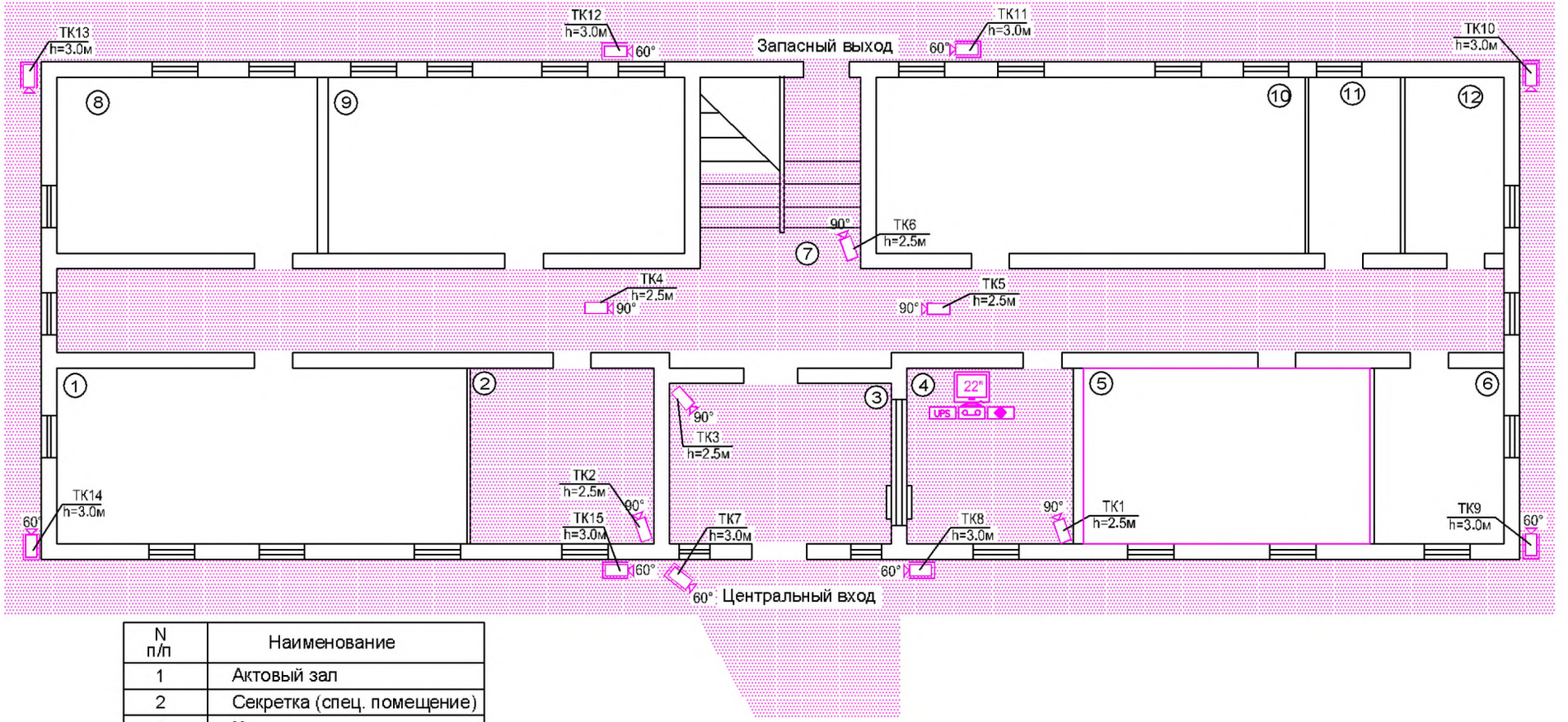


ЭКСПЛИКАЦИЯ ПОМЕЩЕНИЙ

	НАИМЕНОВАНИЕ
1	ПОМЕЩЕНИЕ ОХРАНЫ
2	КОРИДОР
3	САНУЗЕЛ

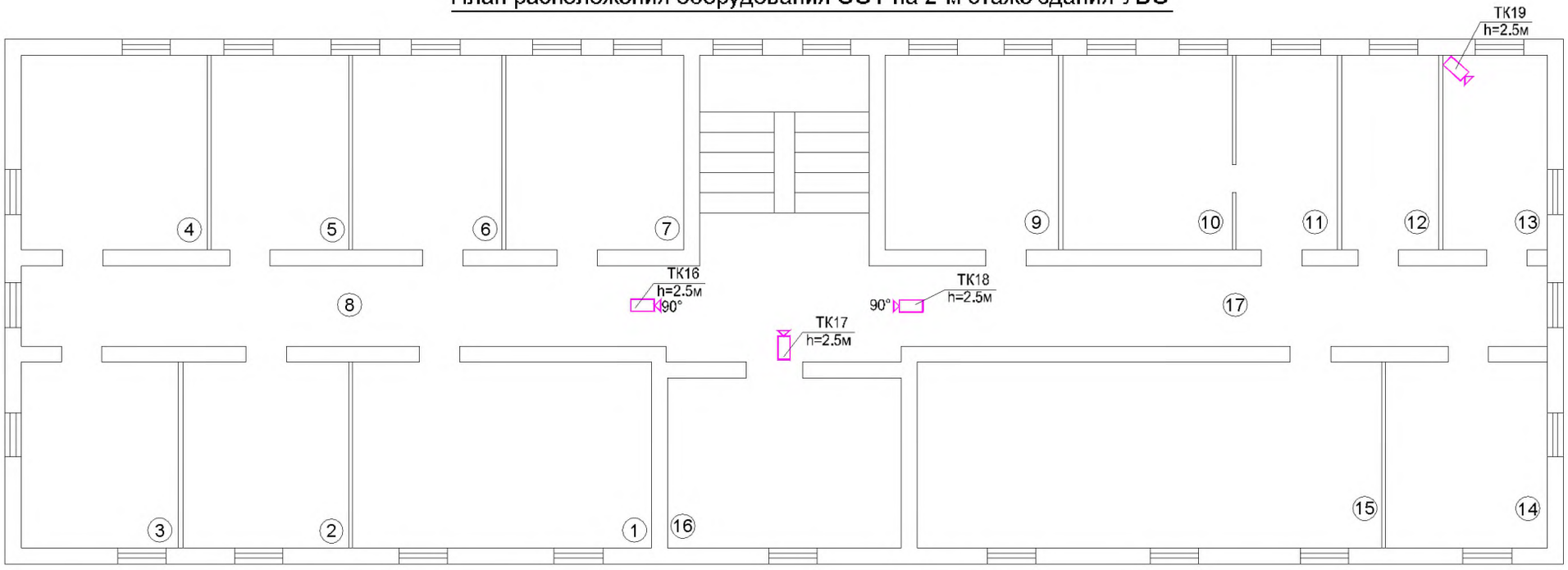
Приложение 4

План расположения оборудования СОТ на 1-м этаже здания УВО



N п/п	Наименование
1	Актовый зал
2	Секретка (спец. помещение)
3	Холл
4	Помещение охраны
5	Секретариат
6	Кабинет
7	Коридор
8	Кабинет
9	Кабинет
10	Архив
11	Сан.узел мужской
12	Сан.узел женский

План расположения оборудования СОТ на 2-м этаже здания УВО



N п/п	Наименование	N п/п	Наименование
1	Кабинет	10	Кабинет начальника
2	Кабинет	11	Приемная
3	Кабинет	12	Кабинет
4	Кабинет	13	Спецпомещение
5	Кабинет	14	Кабинет
6	Группа кадров	15	Учебный класс
7	Группа кадров	16	Кабинет
8	Коридор	17	Коридор
9	Юристконсульт		

Схема структурная СОТ здания УВО

СОТ построена с использованием сетеых телевизионных камер с передачей электропитания PoE.

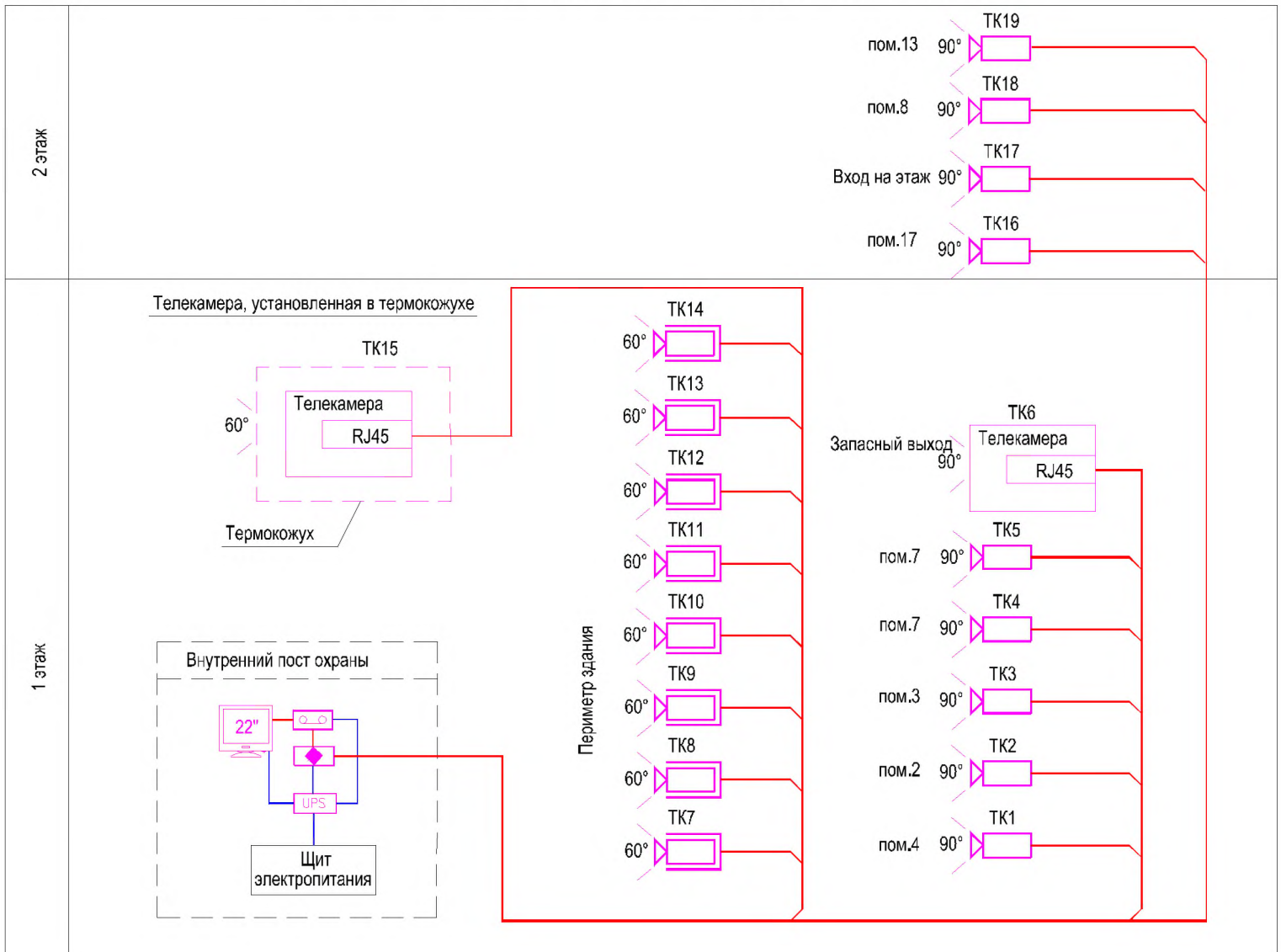
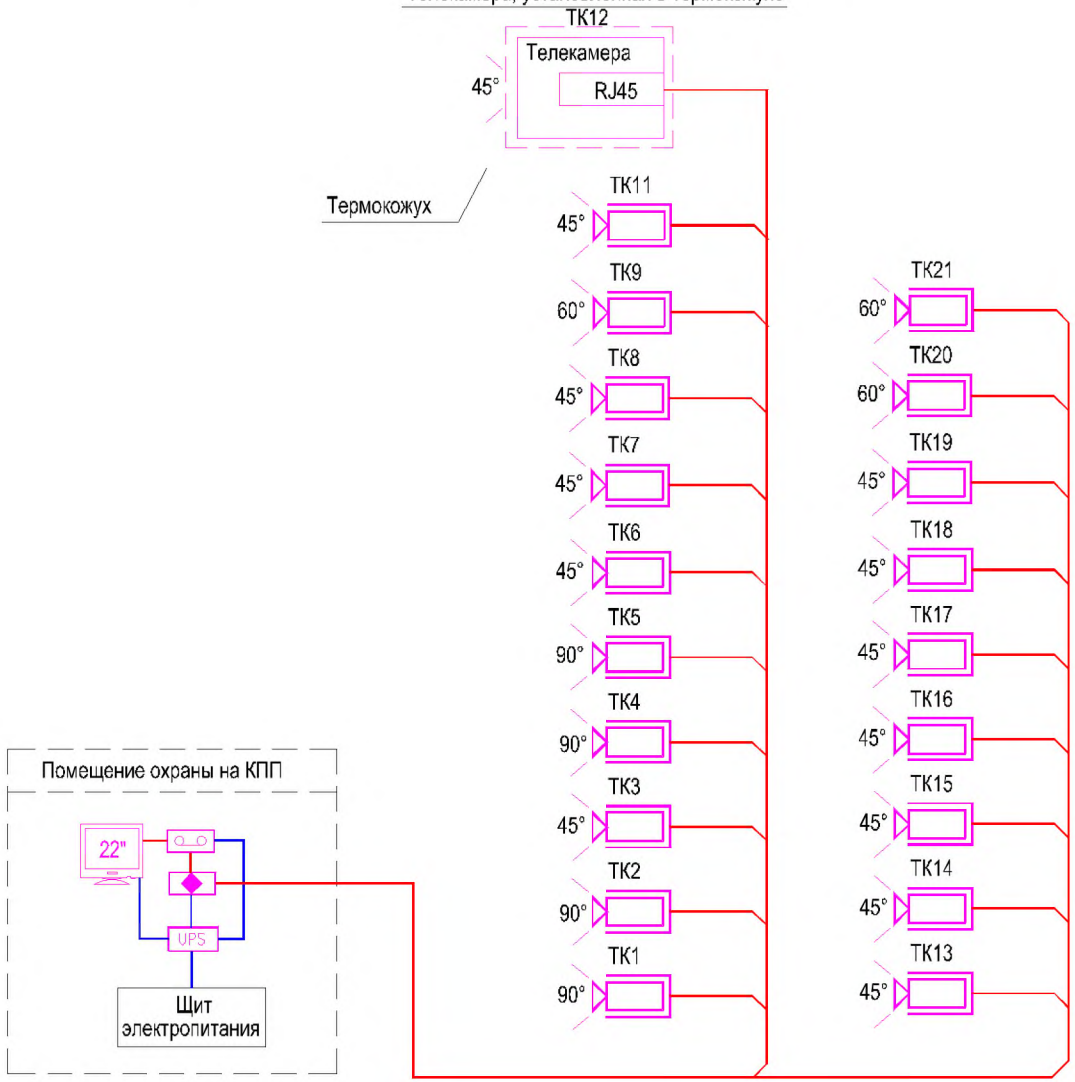
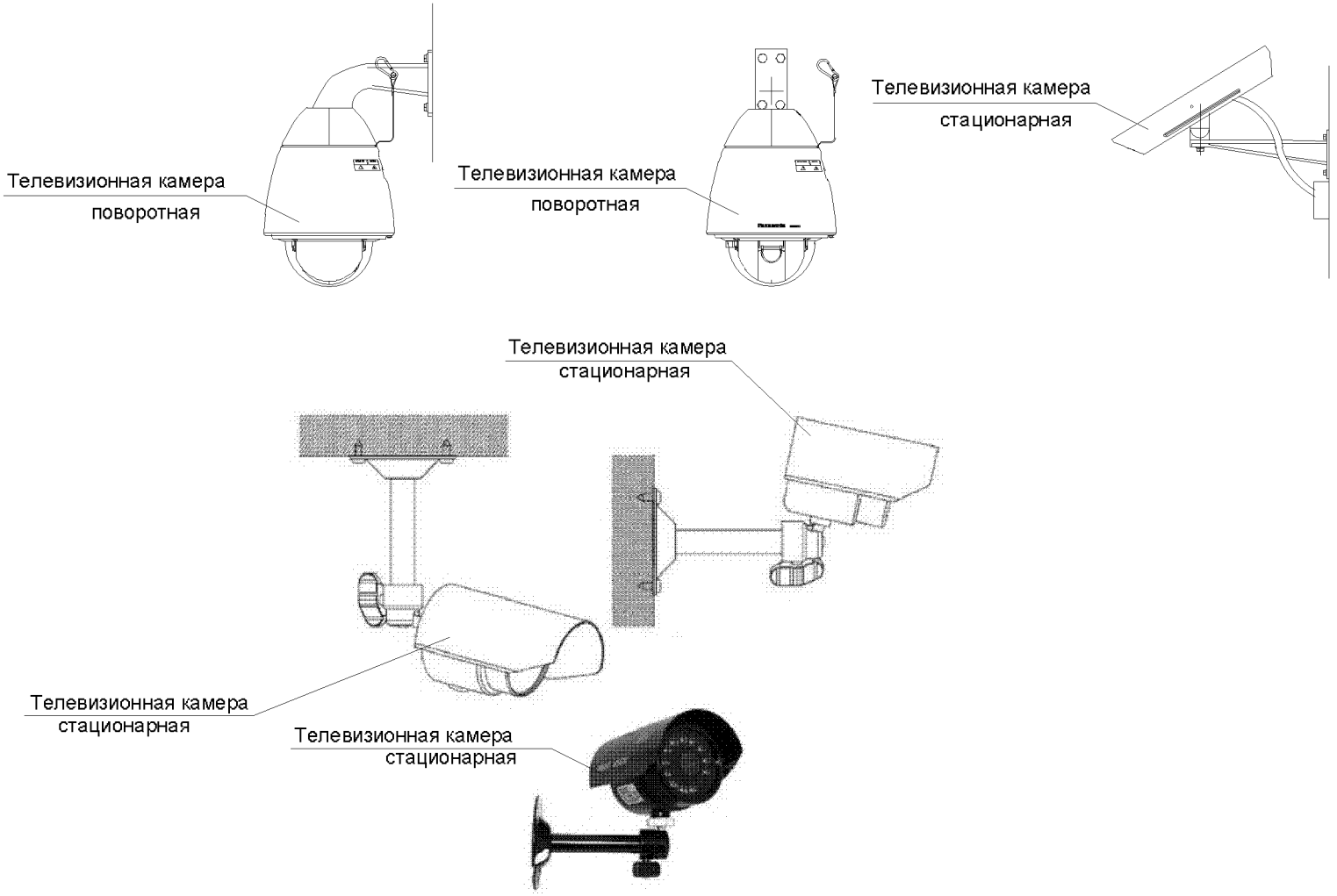


Схема структурная СОТ периметра территории

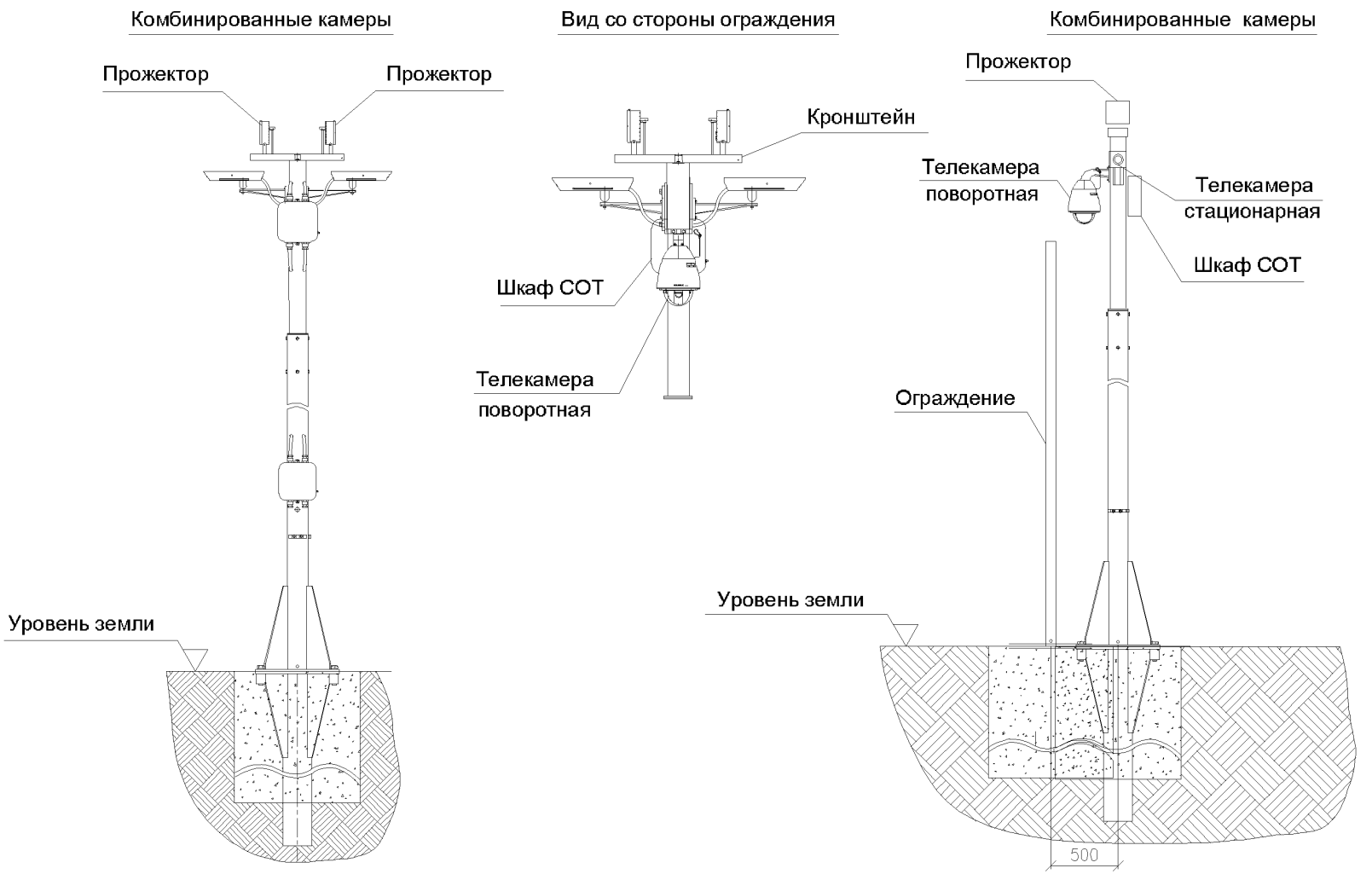
СОТ построена с использованием сетеых телевизионных камер с передачей электропитания PoE.



Схемы установки телевизионных камер на стене и потолке



Схемы установки телевизионных камер на столбах



ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к третьей категории»

Система контроля и управления доступом

РАЗДЕЛ 4

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	148
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	149
3.	СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ (СКУД)	150
3.1.	Типы и виды СКУД их назначение и функции	150
3.2.	Функции СКУД в составе систем противокриминальной защиты объектов	150
3.3	Классификация СКУД	152
3.4	Составляющие СКУД	154
3.5	Электропитание СКУД	161
3.6	Выбор СКУД для оборудования объекта	162
3.7	Размещение и монтаж СКУД	163
3.8	Требования к минимально необходимому составу СКУД	165

ПРИЛОЖЕНИЯ

Приложение 1.	Условные обозначения.	169
Приложение 2.	План расположения оборудования СКУД 1-го этажа.	170
Приложение 3.	План расположения оборудования СКУД 2-го этажа.	171
Приложение 4.	СКУД здания КПП.	172
Приложение 5.	Схема установки средств СКУД на одностворчатой двери.	173
Приложение 6.	Схема установки средств СКУД на двустворчатой двери.	174

1. ОБЩАЯ ЧАСТЬ.

Методические рекомендации по оснащению ведомственных объектов СКУД разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 2.01.2013 № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;

- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- Р 78.36.005-2011 «Выбор и применение систем контроля и управления доступом»;
- Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- РД 78.145-93 «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приёмки работ»;
- Пособие к РД 78.145-93;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану: Методические рекомендации»;
- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ - Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА.

В соответствии с пунктом 4.3 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом III категории по степени потенциальной угрозы понимается отдельно стоящие здания или сооружения, имеющие прилегающую территорию (или без таковой), на которых осуществление

круглосуточного пропускного режима и круглосуточного дежурства не обязательно.

3. СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ.

Система контроля и управления доступом – совокупность программно-технических средств и организационно-методических мероприятий для санкционированного доступа в помещения (зоны) охраняемого объекта и регистрации фактов доступа и попыток несанкционированного доступа, а также оперативный контроль за санкционированным доступом на территории охраняемого объекта.

3.1 Типы и виды СКУД. Их назначение и функции.

СКУД классифицируются по:

- способу управления;
- количеству контролируемых точек доступа;
- функциональным характеристикам;
- уровню защищённости системы от несанкционированного доступа к информации.

По способу управления СКУД различают:

- автономные – для управления одним или несколькими устройствами преграждающими управляемыми (УПУ), без передачи информации на центральное устройство управления и без контроля со стороны оператора;
- централизованные (сетевые) – для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;
- универсальные (сетевые) – включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи.

По количеству контролируемых точек доступа:

- малой ёмкости (до 64 точек);
- средней ёмкости (от 64 до 256 точек);
- большой ёмкости (более 256 точек).

По функциональным характеристикам СКУД могут быть трёх классов:

1 - системы с ограниченными функциями;

2 - системы с расширенными функциями;

3 - многофункциональные системы.

Классификация средств и систем контроля и управления доступом по устойчивости к несанкционированным действиям (далее НСД).

Классификация средств СКУД по устойчивости к НСД определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости:

- нормальной;
- повышенной;
- высокой.

УПУ классифицируют по устойчивости к разрушающим воздействиям.

Устойчивость УПУ устанавливается по:

- устойчивости к взлому;
- пулестойкости (только для УПУ со сплошным перекрытием проема);
- устойчивости к взрыву.

Нормальная устойчивость УПУ обеспечивается механической прочностью конструкции без оценки по показателям устойчивости к разрушающим воздействиям.

Для УПУ повышенной и высокой устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и с блокированием объекта в проеме (шлюзы, кабины проходные) устанавливается классификация по устойчивости к взлому, взрыву и пулестойкости.

Устройства исполнительные (замки, защелки) классифицируют по устойчивости к разрушающим воздействиям в зависимости от конструкции.

По устойчивости к неразрушающим воздействиям средства КУД в зависимости от их функционального назначения классифицируют по следующим показателям:

- устойчивости к вскрытию - для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивости к манипулированию;
- устойчивости к наблюдению для считывателей ввода запоминаемого кода (клавиатуры, кодовые переключатели и т.п);
- устойчивость к копированию (для идентификаторов);
- устойчивости защиты средств вычислительной техники (СВТ) средств управления СКУД от несанкционированного доступа к информации.

Классификация систем КУД к НСД определяется для систем с централизованным управлением по защищенности от несанкционированного доступа к информации программного обеспечения СКУД и средств СВТ, входящих в состав сетевых СКУД.

3.2 Функции СКУД в составе систем противокриминальной защиты объектов.

СКУД применяются для предотвращения несанкционированного доступа людей, транспорта и других объектов в зону (из зоны) доступа (здания, помещения, территории, транспортные средства) в целях обеспечения противокриминальной защиты объектов.

СКУД действуют по принципу сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту, с информацией, заложенной в памяти системы.

СКУД должна выполнять следующие функции:

санкционирование – процедура присвоения каждому пользователю персонального идентификатора, кода, регистрацию его в системе (или регистрацию его биометрических признаков) и задание для него временных интервалов и уровня доступа (в какие помещения, когда и кто имеет право заходить);

идентификацию – процедуру опознавания пользователя по предъявленному идентификатору или биометрическому признаку;

авторизацию – проверку полномочий, заключающуюся в проверке соответствия времени и уровня доступа установленным в процессе санкционирования;

аутентификацию – установление подлинности пользователя по признакам идентификации;

разрешение доступа или отказ в доступе – выполняется на основании результатов анализа предыдущих процедур;

регистрация – протоколирование всех действий в системе;

реагирование – реакция системы на несанкционированные действия (подача предупреждающих и тревожных сигналов, отказ в доступе и т.д.).

3.3 Классификация СКУД.

1-й класс - системы с ограниченными функциями.

К СКУД 1-го класса относятся малофункциональные системы малой ёмкости, работающие в автономном режиме. Такие системы применяются в случае, если на объекте необходимо обеспечить контролируемый доступ сотрудников и посетителей, имеющих соответствующий идентификатор. При этом не ставится задача контроля времени доступа и выхода из помещения, регистрация проходов, передача данных на центральный компьютер.

Автономная система состоит из контроллера, обычно объединённого со считывателем, и исполнительного элемента. Как правило, используются магнитные (реже бесконтактные) карточки, электронные ключи "TouchMemory". В зависимости от типа контроллера количество лиц в списках может достигать от 60 до 2800 человек. Автономные системы снабжаются резервным питанием и имеют механический ключ для открывания замка в аварийных ситуациях.

Устанавливаются на объектах, где требуется только ограничение доступа посторонних лиц (функция замка).

2-й класс - системы с расширенными функциями.

СКУД 2-го класса – монофункциональные системы (одноуровневые и многоуровневые системы, работающие в автономном или сетевых режимах).

СКУД малой и средней емкости, но с возможностью расширения и включения их или их составных частей в общую линию связи (сетевой режим).

Данные системы имеют ряд дополнительных функций:

– ограничение допуска в охраняемую зону конкретного лица, группы лиц по дате и временным интервалам в соответствии с имеющимся идентификатором;

– автоматическую регистрацию событий в собственном буфере памяти, выдачу тревожных извещений (при несанкционированном проникновении, неправильном наборе кода или взломе заграждающего устройства или его элементов) на внешние оповещатели или внутренний пост охраны;

– автоматическое управление открытием/закрытием устройства заграждения.

Устанавливаются на объектах, где требуется учёт и контроль присутствия сотрудников в разрешённой зоне, в качестве дополнения к имеющимся на объекте системам охраны и защиты.

На объектах, оборудованных средствами и системами охранно-пожарной сигнализации (ОПС), СКУД 2-го класса применяются как самостоятельные системы, и они часто рассматриваются только как средства усиления режима обеспечения безопасности объекта.

3-й класс – многофункциональные системы.

СКУД 3-го класса (сетевые). Контроллеры систем данного класса объединены в локальную сеть, работающую в реальном времени и ведущую непрерывный диалог с периферийными устройствами, с ведущим контроллером или с управляющим компьютером, расположенным в пункте охраны. Системы этих классов – крупные многоуровневые системы, рассчитанные на большое число пользователей (1500 человек и более).

Подобные системы применяются в случае, когда необходимо контролировать время прохода сотрудников и посетителей на объект и в помещения. При этом применяются более сложные электронные идентификаторы (Proximity, Виганд карточки, биометрический контроль или их сочетание). Время прохода на каждый день недели и для каждого владельца электронной карточки задаётся администратором системы.

Системы 3-го класса обычно интегрируются с системами охранно-пожарной сигнализации и системами телевизионного наблюдения на релейном уровне. Релейный уровень предполагает наличие дополнительного модуля в контроллере (или дополнительных входов/выходов в контроллере), к которому подключаются охранные или пожарные извещатели и релейные выходы для управления телекамерами и другими устройствами. Подобная интеграция применяется, в основном, на малых объектах. На таких объектах количество взаимодействий между системами невелико, и все они могут быть учтены в процессе проектирования системы безопасности. Этот уровень интеграции является простым, универсальным и достаточно надёжным.

3.4 Составляющие СКУД.

Устройства преграждающие управляемые – устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (двери оборудованные исполнительными СКУД).

Устройства исполнительные (УИ) – устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние устройств преграждающих управляемых (электромеханические, электромагнитные замки, электромагнитные защёлки, механизмы привода шлюзов, ворот, турникетов и другие подобные устройства).

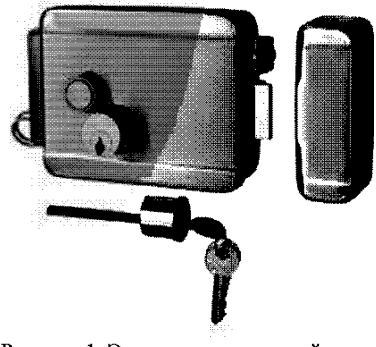


Рисунок 1. Электромеханический замок.

Электромеханический принцип действия исполнительного механизма замка основан на перемещении закрывающих элементов (запоров, ригелей замков и т.п.) с помощью включения на время их передвижения электромотора или электромагнита (Рисунок 1).

В исполнительных механизмах с электромагнитным принципом действия отсутствуют движущиеся механические закрывающие элементы, то есть блокировка устройств заграждения (например, дверей) осуществляется с помощью сил магнитного притяжения, создаваемых мощным магнитом.

Часто в электромеханических замках применяют электромагнитную блокировку (магнитные защёлки, задвижки и т.п.) закрывающих элементов с возможностью перемещения их вручную при открывании или закрывании в экстремальных условиях.

Электромеханический замок рекомендуется устанавливать на деревянных и/или металлических дверях массой до 100 кг при условии средней нагруженности (100 – 200 проходов в день). Применение этого замка для дверей с высокой нагруженностью неэффективно из-за высокого механического износа и, как следствие, снижения надёжности и срока службы. Чаще всего электромеханический замок устанавливают на двери (накладной или врезной замок), но иногда его устанавливают и на дверной коробке.

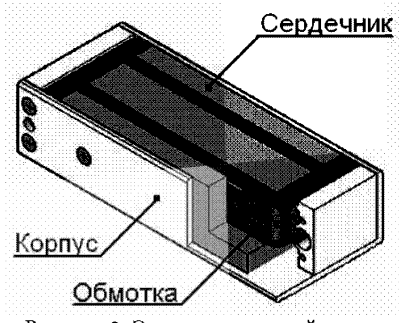


Рисунок 2. Электромагнитный замок.

Электромагнитный замок (Рисунок 2) рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг при условии высокой нагруженности (более 200 проходов в день). Отсутствие деталей, подверженных трению и износу, делает этот замок практически вечным.

Особенностью данного замка является необходимость постоянной подачи тока на обмотку электромагнита, при пропадании напряжения в сети (например, при аварии или умышленном обрыве проводов) замок открывается. В связи с этим для надёжной работы необходимо дублировать электромагнитный замок механическим или применять дополнительное резервное питание.

Электромагнитную защёлку рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери (при ее закрывании), и разблокировать замок при подаче сигнала управления на открывание двери. Такая установка защёлки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромагнитные замки с плоским якорем выпускают двух видов: с якорем, работающим на отрыв, и с якорем, работающим на сдвиг. В обесточенном состоянии все замки нормально открыты. Замки с якорем "на отрыв" изготавливают в накладном варианте, а с якорем "на сдвиг" – в накладном и врезном вариантах.

Для входных дверей используют электромагнитные замки с силой удержания от 200 до 600 кг, при этом ток потребления таких замков (при напряжении питания 12 В) составляет от 200 до 500 мА.

Помимо прямоугольных электромагнитных замков освоен выпуск круглых замков. Это позволило упростить изготовление и снизить стоимость. К недостаткам электромагнитных замков следует отнести потерю работоспособности при образовании зазора между электромагнитом и пластиной. Во избежание такой ситуации пластину укрепляют на резиновой прокладке, компенсирующей образующийся зазор.

Требование обеспечения соприкосновения электромагнита и пластины без зазора для обеспечения работоспособности замка, вызывает

необходимость обязательного применения качественного дверного доводчика.

Функция доводчика – не только гарантировать закрытие двери, но также оберегать замок от механических ударов.

Электромагнитные замки с плоским якорем имеют очень высокую надёжность, это определяется, в основном, конструкцией замка и в значительной степени – отсутствием трущихся деталей, износ которых ограничивает долговечность. Ударные нагрузки, возникающие при закрывании двери (особенно, если дверной доводчик плохо отрегулирован), и перепады температуры создают тяжёлые условия для элементов электроники. Поэтому их размещают вне корпуса замка.

Устройства считывающие (УС).

УС – это устройство, предназначенное для считывания (ввода) идентификационных признаков с целью опознания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. По принципу считывания они могут быть:

- с ручным вводом;
- контактные;
- бесконтактные;
- биометрические;
- комбинированные.

Идентификаторы (ИД) (носитель идентификационного признака).

Идентификатор – это уникальный признак субъекта или объекта. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код – предмет, в котором (на который) с помощью специальной технологии занесён идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и другие устройства).

Разновидности идентификаторов.

Механические – представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей).

К механическим идентификаторам относятся такие устройства, как кодовые панели и механические ключи. Механические идентификаторы просты и имеют несколько недостатков: простота подделки, наличие движущихся частей, которые снижают надёжность, невозможность использования для идентификации личности.

Магнитные – представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда) (Рисунок 3).

Данная технология получила широкое распространение в системах контроля и управления доступом благодаря относительной сложности подделки идентификаторов, возможности применения карт в качестве

идентификаторов личности. Магнитные системы позволяют разграничивать доступ для большого числа пользователей (до 2000 и более).

Оптические – представляют собой нанесённые на поверхность или внутри идентификатора метки, имеющие различные оптические характеристики (карты со штрих кодом, голографические метки) (Рисунок 4).

Электронные контактные – представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи) (Рисунок 5).



Рисунок 3. Карта доступа с магнитной полосой.



Рисунок 4. Карта доступа со штрих кодом.



Рисунок 5. Электронная карта доступа.

Электронный ключ TouchMemory представляет собой металлическую "таблетку" небольшого диаметра толщиной 4-6 мм, внутри которой запрессована электронная микросхема с уникальным 48-разрядным кодом. "Таблетка" не имеет собственного источника питания, а заряжается от считывателя при соприкосновении с ним. И ключ, и считыватель

изготавливаются в герметичном исполнении, что делает их практически вечными. Они надёжны в работе, имеют высокую устойчивость к электромагнитным и криминальным воздействиям. Для удобства пользования "таблетка" закрепляется в пластмассовой пластинке, имеющей отверстие для подвешивания её на одну связку с другими ключами (Рисунок 6).



Рисунок 6. Электронные ключи TouchMemory.

Карточка бесконтактная (Proximity) – карточка, с которой информация о коде ключа считывается радиочастотным способом на расстоянии (то есть без непосредственного контакта со считывателем). Различают пассивные и активные карточки. Пассивные карточки питаются энергией, получаемой от считывателя, и действуют на расстоянии до 10 см (Рисунок 7).



Рисунок 7. Карточка бесконтактная (Proximity).

Активные – имеют встроенную батарейку, срок работы которой составляет до 10 лет. Считыватель размещается, как правило, скрытно в полости неметаллической двери или за радиопрозрачной стенкой. В пассивных карточках информация записывается один раз на всё время действия карточки, а в активных существует возможность ее изменения.

Электронные радиочастотные – считывание кода с электронных идентификаторов происходит путём передачи данных по радиоканалу.

Акустические – представляют собой кодированный акустический сигнал.

Средства управления (аппаратные устройства).

Контроллер доступа (КД) и прибор приемно-контрольный доступа (ППКД) представляют собой аппаратное устройство в составе средств управления системы контроля и управления доступом (Рисунок 8).

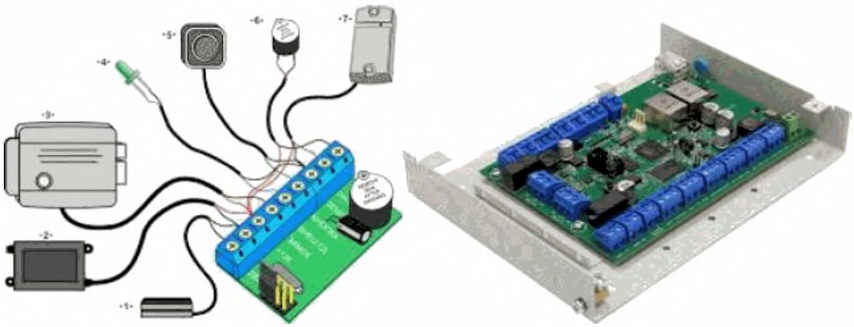


Рисунок 8. Контроллер доступа.

Автономный – для управления одним или несколькими устройствами преграждающими управляемыми без передачи информации на центральное устройство управления и контроля со стороны оператора.

Централизованный (сетевой) – для управления устройствами преграждающими управляемыми с обменом информацией с центральным пультом и контролем управления системой со стороны центрального устройства управления.

Универсальный (сетевой) – включает в себя функции как автономных, так и сетевых систем, работающих в сетевом режиме под управлением центрального устройства управления, переходящий в автономный режим при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи.

Домофоны.

Домофон – устройство для управления доступом с возможностью дистанционного управления сотрудником дежурной смены на основе получаемой аудио/видеоинформации (Рисунок 9).

Домофоны сочетают в себе функции аудио- и/или видеоконтроля и управления доступом на объекте. Домофоны позволяют абоненту, не подходя к двери, идентифицировать посетителя по изображению и/или голосу и дистанционно управлять входной дверью.

Домофон позволяет, соблюдая безопасную дистанцию между посетителем и охраной объекта, выяснить требующуюся информацию о посетителе и принять взвешенное решение о его допуске на объект.

При выборе домофона необходимо обращать особое внимание на его климатическое исполнение, антивандальные свойства, надёжность.



Рисунок 9. Домофоны.

По виду (способу идентификации посетителей) домофоны подразделяются на:

Аудиодомофоны обеспечивают двухстороннюю аудиосвязь абонента с посетителем и позволяют идентифицировать посетителя по его голосу.

Видеодомофоны обеспечивают видеоконтроль наружного околодверного пространства, двухстороннюю аудиосвязь абонента с посетителем и позволяют идентифицировать посетителя по его изображению и голосу.

По количеству обслуживаемых абонентов различают:

Индивидуальные (одноабонентские) – домофоны позволяют обслуживать только одного абонента и применяют для защиты отдельных квартир, небольших офисов, загородных домов, а также могут быть установлены на постах охраны.

Видеодомофон обеспечивает более высокий уровень безопасности абонента, чем аудиодомофон, так как (помимо двухсторонней аудиосвязи) позволяет получить телевизионное изображение посетителя.

При выборе домофона следует обращать особое внимание на такие факторы:

- климатическая устойчивость, прежде всего – диапазон рабочих температур, который должен быть для некоторых блоков (например, блока вызова, электрозамка, доводчика двери) не менее минус 40÷плюс 40° С;
- устойчивость к вандализму;
- устойчивость к нестабильному электропитанию;
- наличие сертификата соответствия;
- обязательное наличие полной эксплуатационной документации с принципиальными и монтажными схемами на русском языке;
- наличие стабильного гарантийного и послегарантийного обслуживания предлагаемого оборудования и возможность закупки ремонтных ЗИП.

3.5 Электропитание СКУД.

Основное электропитание СКУД должно осуществляться от сети переменного тока частотой 50 Гц номинальным напряжением 220 В.

СКУД должна быть работоспособна при допустимых отклонениях напряжения сети от минус 15% до плюс 10%.

Электропитание отдельных средств СКУД допускается осуществлять от других источников с иными параметрами выходных напряжений, требования к которым устанавливают в нормативных документах на СКУД конкретных типов.

СКУД должны быть обеспечены резервным электропитанием при пропадании напряжения основного источника электропитания.

В качестве резервного источника электропитания может использоваться резервная сеть переменного тока или источники постоянного тока.

Переход на резервное электропитание должен осуществляться автоматически без нарушения установленных режимов работы и функционального состояния средств СКУД.

Резервный источник электропитания должен обеспечивать выполнение основных функций системы при пропадании напряжения в сети:

Системы 1 класса – 0,5 ч.

Системы 2 класса – 0,5 ч.

Система 3 класса – 1 ч.

Допускается не применять резервирование электропитания с помощью аккумуляторных батарей для УПУ, которые требуют для управления значительных мощностей приводных механизмов (приводы ворот, шлюзы).

При этом такие УПУ должны быть оборудованы аварийными механическими средствами открывания и системными средствами индикации аварии электропитания.

При использовании в качестве источника резервного электропитания СКУД аккумуляторных или сухих батарей рекомендуется иметь индикацию разряда батареи ниже допустимого предела.

Химические источники электропитания, встроенные индикаторы или обеспечивающие сохранность данных в контроллерах, должны обеспечивать работоспособность СКУД в течение не менее трёх лет.

3.6 Выбор СКУД для оборудования объекта.

Выбор варианта оборудования объекта средствами СКУД следует начинать с его обследования.

Целью обследования является определение размера возможного ущерба предприятию (организации) или собственнику имущества и связанной с ним категории объекта.

По результатам обследования определяются тактические характеристики и структура СКУД, а также составляется техническое задание на оборудование объекта СКУД. В техническом задании указывается:

- назначение СКУД, техническое обоснование и описание системы;
- размещение составных частей системы;
- условия эксплуатации средств СКУД;
- основные технические характеристики, такие, как:
  - пропускная способность в охраняемые зоны, особенно в час-пик;
  - максимально возможное число пользователей на один считыватель;
  - максимальное число и виды идентификаторов;
  - требования к маскировке и защите средств СКУД от вандализма;
- оповещение о тревожных и аварийных ситуациях и принятие соответствующих мер по их пресечению или предупреждению;
- возможность работы и сохранения данных без компьютера или при его отказе;
- алгоритм работы системы СКУД в аварийных и чрезвычайных ситуациях;
- программное обеспечение системы;
- требования к безопасности;
- требования к электропитанию;
- обслуживание и ремонт системы;
- требования к возможности включения системы СКУД в интегрированную систему безопасности.

Путём изучения чертежей, обхода и осмотра объекта, а также проведения необходимых измерений определяются:

- количество входов/выходов и их геометрические размеры (площадь, линейные размеры, пропускная способность и т.п.);
- материал строительных конструкций;
- количество отдельно стоящих зданий, их этажность;
- количество открытых площадок;
- количество отапливаемых и неотапливаемых помещений и их расположение.

Учитывать вредное воздействие окружающей среды следует лишь для исполнительных устройств, считывателей и контроллеров (совмещенных со считывателями в одном конструктивном блоке), предназначенных для работы вне отапливаемых закрытых помещений либо в особых условиях (запылённость, повышенная влажность, отрицательная температура, агрессивная среда и т. п.). Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, удалённость считывателей и контроллеров от управляющего центра, заземление составных частей системы и т.п.

3.7 Размещение и монтаж СКУД

Устройства центрального управления.

Устройства центрального управления (персональные компьютеры), являющиеся "мозгом" СКУД, рекомендуется устанавливать в отдельных служебных помещениях, защищённых от доступа посторонних лиц, например, в помещении дежурной части.

Основные положения, в соответствии с которыми разрабатываются режимы работы всей системы безопасности, определяются руководящим составом объекта, исходя из общей концепции обеспечения безопасности объекта. Управляющие программы загружаются в центральный управляющий и вспомогательные компьютеры или контроллеры и защищаются секретными кодами.

Персонал охраны, а также других служб, которые подключены к общей компьютерной сети, не должны иметь доступа к программным средствам и возможности влиять на установленные режимы работы, за исключением лиц, ответственных за данные работы.

При объединении компьютеров в сеть целесообразно разделять функциональные возможности среди пользователей сети и в соответствии с этим размещать компьютеры в помещениях объекта.

Устройства контроля и управления.

Ведущие контроллеры и контроллеры, работающие на несколько устройств заграждения, рекомендуется размещать в специальных запираемых металлических шкафах или нишах, на высоте, удобной для технического обслуживания. При этом следует дверцы данных шкафов или ниш блокировать охранной сигнализацией на возможное открытие или пролом.

Корпус данных контроллеров должен быть выполнен из ударопрочного материала, защищающего контроллер от актов вандализма. Контроллеры, управляющие работой считывателей или исполнительных устройств одной двери в двух направлениях, рекомендуется устанавливать с внутренней стороны охраняемого помещения.

При работе устройств контроля и управления в сетевом режиме необходимо учитывать возможность появления помех и сбоев в работе из-за неправильного монтажа соединительных линий и их длины.

Для нормальной работы рекомендуется:

– при значительной длине соединительного кабеля подключать к шине оконечные и согласующие элементы. Необходимое точное значение величины этих элементов зависит от характеристик кабеля;

– заземлять устройства и экранированные оплётки кабелей в одной точке (во избежание возникновения блуждающих токов), желательно у ведущего контроллера. При большой длине кабелей заземление можно производить в разных точках, но при этом обязательно использовать специальные методы и устройства защиты от помех;

– использовать шинные усилители при большой длине кабеля.

Считыватели и устройства исполнительные.

В зависимости от типа считывателей и устройств исполнительных, пропускной способности и организации системы безопасности объекта в целом, они могут устанавливаться как вблизи устройств заграждения, так и непосредственно на них. При их размещении необходимо учитывать условия эксплуатации, удобство монтажа, надёжность и вандалостойкость.

Считыватели "Proximity" удобнее всего размещать на стене, скрытно в стене перед устройствами заграждения или с внутренней стороны устройства заграждения, например, на внутренней стороне неметаллической двери, если её толщина не превышает 10 см.

При монтаже считывателя на металле рекомендуется, чтобы между основанием считывателя и металлической поверхностью расстояние было не менее 25 мм. В случае, когда стена, за которой установлен считыватель, оказывается слишком толстой или изготовлена из металла (содержит металлическую арматуру), считыватель допускается устанавливать на расстоянии, на котором должна быть обеспечена необходимая защита от возможного несанкционированного прохода.

Считыватели магнитных, Виганд карточек, электронных ключей и клавиатуры также рекомендуется размещать на стене или непосредственно на устройстве заграждения на высоте, удобной для пользования.

Считыватели магнитных карточек (за исключением совмещённых с исполнительными устройствами) во избежание помех или даже выхода из строя не рекомендуется устанавливать в непосредственной близости от мощных исполнительных устройств, создающих сильные электромагнитные поля (соленоидные, магнитные замки и т.п.).

Электромагнитные защёлки рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери, при закрывании двери и разблокировать замок при подаче сигнала от контроллера. Кроме того, такая установка защёлки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромеханические замки рекомендуется устанавливать на деревянных и металлических дверях массой до 100 кг при условии средней загруженности (до 100 – 200 проходов в день). Применение этих замков для дверей с высокой загруженностью неэффективно по причине высокого механического износа и как следствие снижения надёжности и срока службы. Чаще всего электромеханические замки устанавливают на двери (накладной или врезной замок), но иногда эти замки устанавливаются и на дверной коробке.

Электромагнитные замки рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг в условиях высокой загруженности (более 200 проходов в день). Отсутствие деталей, подверженных трению и износу, делает этот замок практически вечным. Особенностью данного замка является необходимость постоянной подачи тока на обмотку его электромагнита, так как при пропадании напряжения питания, например, при аварии или умышленном обрыве проводов, замок открывается. В связи с этим для надёжной работы необходимо дублирование его механическим замком или применение дополнительного резервного электропитания.

При совместном использовании магнитоконтактных извещателей в качестве датчиков положения двери с электромагнитными и электромеханическими замками, они должны быть разнесены друг от друга как можно дальше.

При установке исполнительных устройств (замки, доводчики, приводы и т.п.), требующих для своей работы подводки электропитания, необходимо использовать специальные устройства и кабели, обеспечивающие электро- и пожаробезопасность (особенно на сгораемых конструкциях), а также защиту от повреждений при открытии/закрытии дверей (гибкие переходы).

3.8 Общие требования к минимально необходимому составу СКУД.

3.8.1 Минимально необходимый состав СКУД.

Объекты органов внутренних дел Российской Федерации, отнесённые к III категории, должны быть оборудованы СКУД.

СКУД оборудуются:

- контрольно-пропускные пункты (КПП);
- проходные;
- специальные помещения объекта.

СКУД на КПП оборудуются (см. приложение 4):

- проход на территорию;
- вход в помещение охраны.

Все входы в помещение КПП, а также управляемые преграждающие конструкции оборудуются замковыми устройствами и средствами охранной сигнализации, которые выдают сигнал тревоги при попытке преодоления нарушителем этих конструкций путём их вскрытия и разрушения.

Устройства управления механизмами открывания, прохода (проезда), охранным освещением, охранным телевидением, оповещением и стационарными средствами досмотра должны быть расположены в помещении КПП или на его наружной стене со стороны охраняемой территории. При этом необходимо исключить доступ к указанным устройствам посторонних лиц.

Допускается для досмотра транспорта снизу и сверху вместо досмотровых эстакад, вышек и ям применять средства охранного телевидения, мониторы которых устанавливаются в кабинах сотрудников КПП.

Для контроля подъезжающего транспорта и прибывающих граждан сплошные ворота и входные двери на территорию объекта должны быть оборудованы смотровыми окошками или «глазками», домофонами, видеодомофонами или телевизионными камерами.

Проходная в здание оборудуется СКУД (см. приложение 2):

– вход в здание;

– вход в помещение дежурной части.

Внутри здания СКУД оборудуются (см. приложение 2, 3):

– специальные помещения.

3.8.2 Технические требования к СКУД.

СКУД должна обеспечивать:

- контроль и управление точками доступа (двери, турникеты, ворота) на вход и выход;
- подключение считывателей электронных кодовых ключей;
- контроль аварийного открывания преграждающих устройств;
- контроль блокировки преграждающих устройств;
- контроль отказа от прохода;
- контроль исправности запорного устройства;
- возможность передачи тревожной информации на автоматизированные рабочие места системы сбора и обработки информации;
- контроль состояния связи с контроллерами системы контроля и управления доступом;
- защиту цепей питания от перенапряжения, переполюсовки и перегрузок;
- защиту входных цепей от перенапряжения и переполюсовки;
- предоставление доступа и идентификацию пользователей, проходящих через точку доступа по электронному ключу или электронной идентификационной карте;

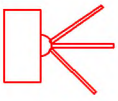
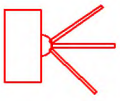
- дистанционное управление (блокирование, разблокирование);
- автономную работу без потери данных в течение не менее 24 ч. при потере связи с автоматизированными рабочими местами;
- глобальный контроль повторного прохода;
- зональный контроль местоположения персонала;
- ведение журнала событий;
- получение отчёта о проходах;
- работу бюро пропусков;
- возможность наращивания количества устройств в процессе эксплуатации;
- контроль и управление доступом сотрудников и посетителей через контрольно-пропускной пункт;
- идентификацию входящих (выходящих) по электронному ключу-идентификатору;
- идентификация (получение разрешения на проход, проезд) должна осуществляться по одному признаку.

Эвакуационные и аварийные выходы должны быть оборудованы устройством экстренного открывания дверей (устройство «Антипаника») по ГОСТ 31471-2011 «Устройства экстренного открывания дверей эвакуационных и аварийных выходов. Технические условия».

«Антипаниковая» дверь – это металлическая дверь, устойчивая к взлому снаружи и оборудованная специальными «антипаниковыми» замками и извещателем на открывание с выводом на КПП.

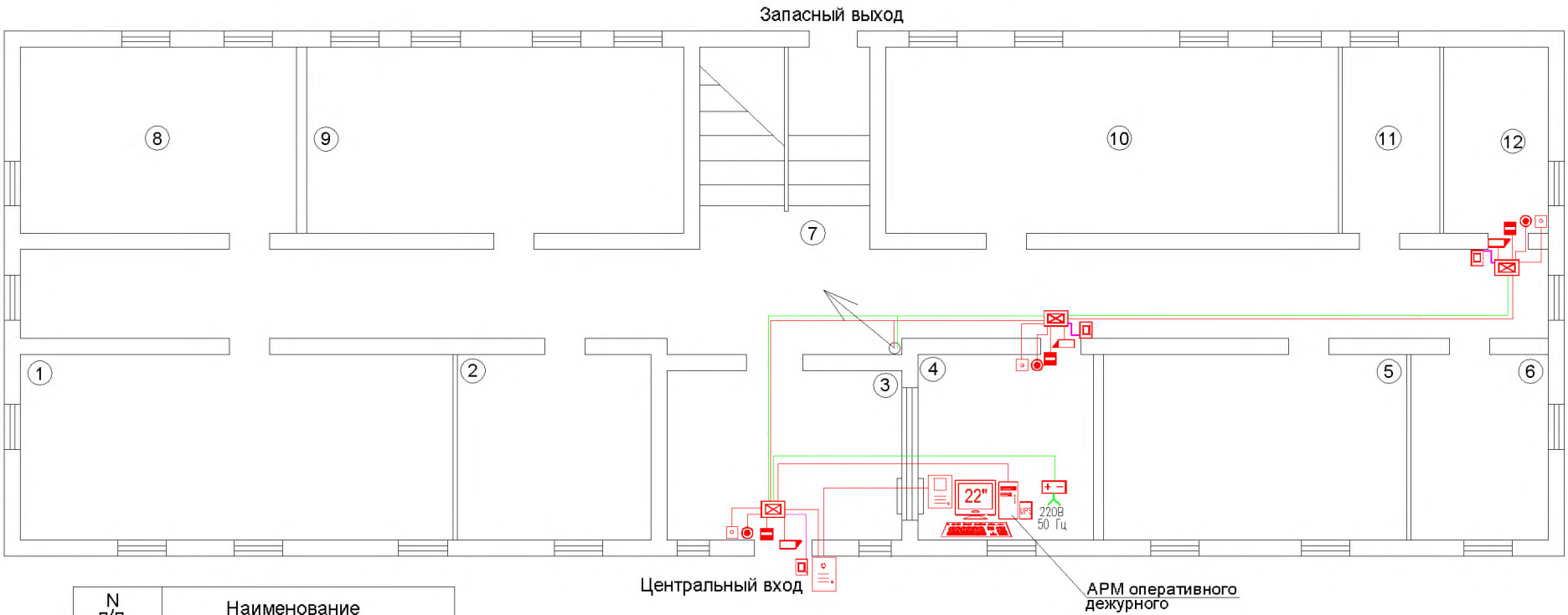
ПРИЛОЖЕНИЯ

Условные обозначения

Наименование	Обозначение	
	на планах	на схемах
АРМ дежурного оператора		
Пульт управления		
Контроллер управления доступом		
Бесконтактный считыватель с клавиатурой		
Извещатель охранный магнитоконтактный		
Кнопка "ВЫХОД"		
Кнопка аварийного разблокировки электромагнитного замка (турникета)		
Электромагнитный замок		
Монитор видеодомофона		
Вызывная панель видеодомофона		
Турникет		
Резервированный источник электропитания питания 12В		
Бесперебойный источник питания		
Блок управления турникетом		
Провод КПСВВнг(А)FRLS1х2х0,5		
Провод КПСВВнг(А)FRLS1х2х1,5		
Провод КПСВЭВнг(А)FRLS2х2х1,5		
Провод UTP4х2х0,5		

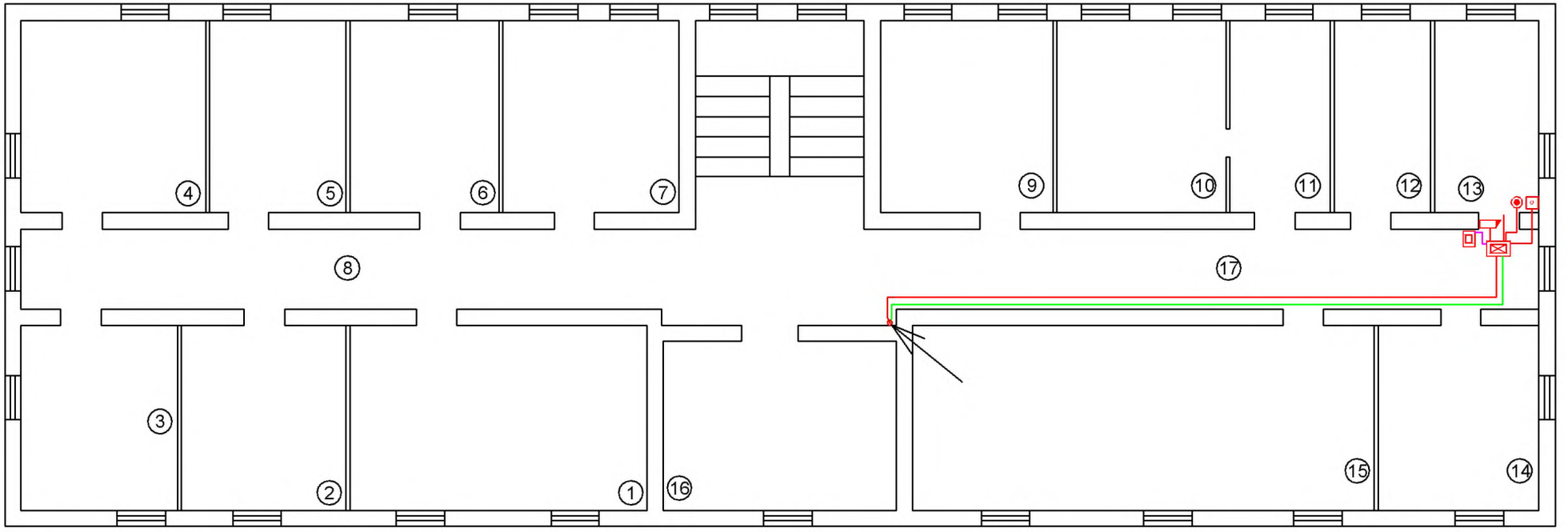
Приложение 2

План расположения оборудования СОТС 1-го этажа здания ОВД



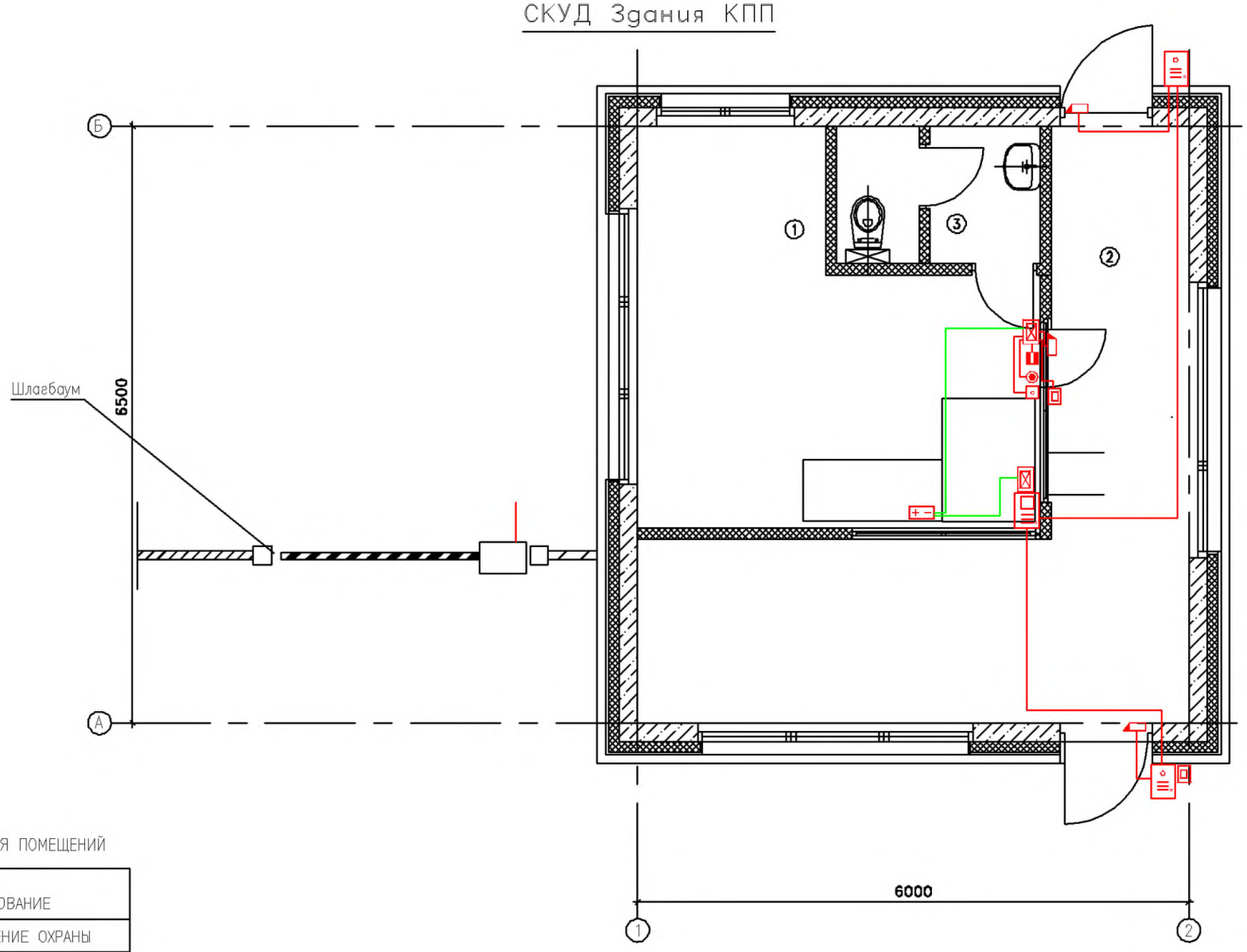
N п/п	Наименование
1	Актовый зал
2	Секретка (спец. помещение)
3	Холл
4	Помещение охраны
5	Секретариат
6	Кабинет
7	Коридор
8	Кабинет
9	Кабинет
10	Архив
11	Сан.узел мужской
12	Сан.узел женский

План расположения оборудования СОТС 2-го этажа здания ОВД



N п/п	Наименование	N п/п	Наименование
1	Кабинет	10	Кабинет начальника
2	Кабинет	11	Приемная
3	Кабинет	12	Кабинет
4	Кабинет	13	Спецпомещение
5	Кабинет	14	Кабинет
6	Группа кадров	15	Учебный класс
7	Группа кадров	16	Кабинет
8	Коридор	17	Коридор
9	Юристконсульт		

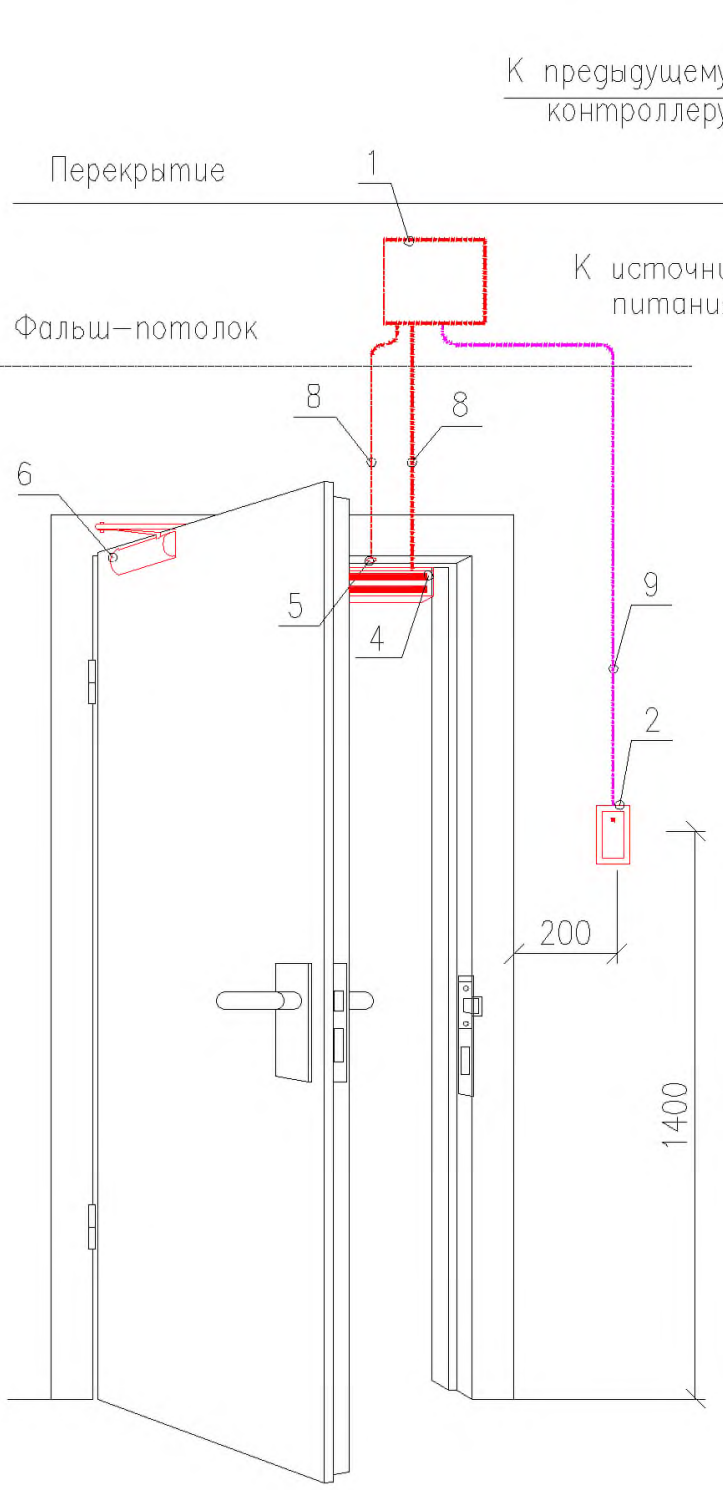
СКУД Здания КПП



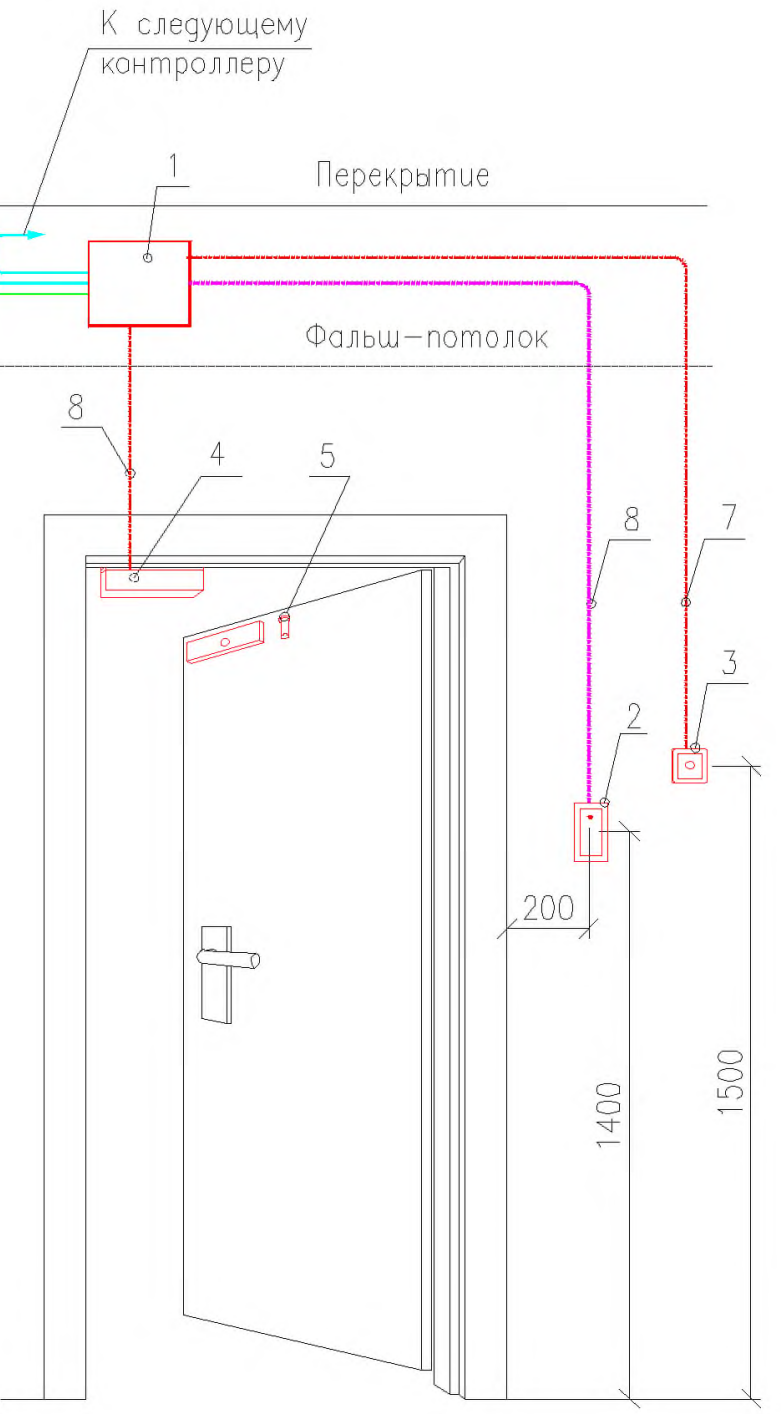
ЭКСПЛИКАЦИЯ ПОМЕЩЕНИЙ

	НАИМЕНОВАНИЕ
1	ПОМЕЩЕНИЕ ОХРАНЫ
2	КОРИДОР
3	САНУЗЕЛ

Схемы установки средств СКУД на одностворчатой двери



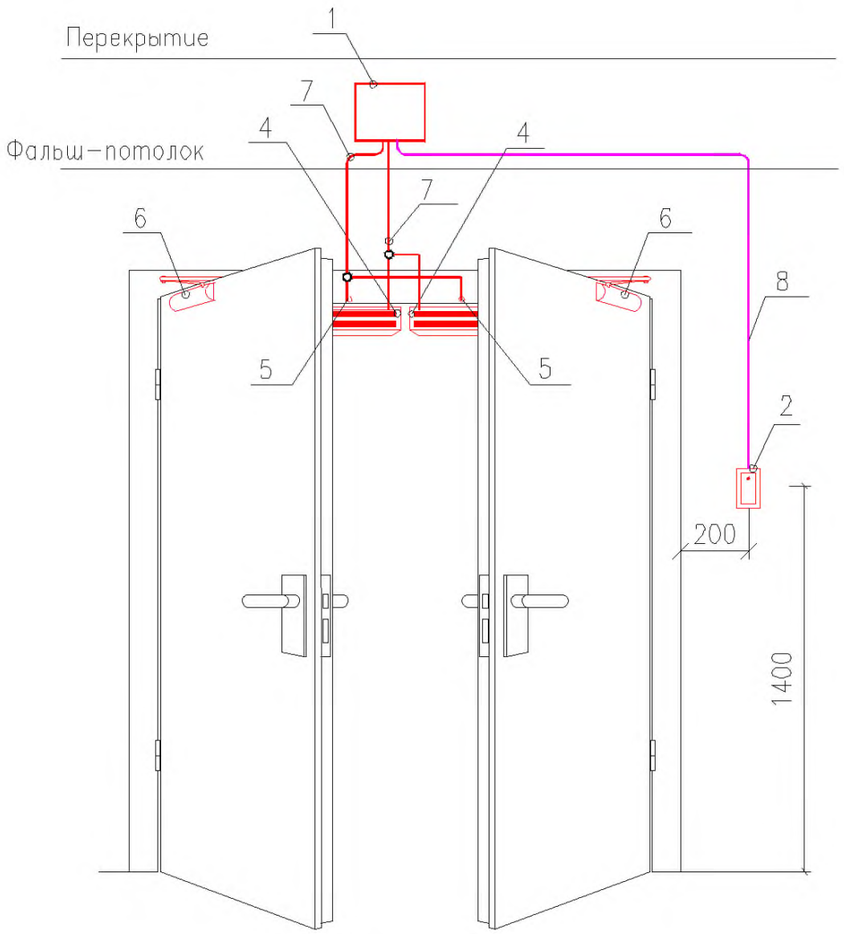
Вид со стороны коридора



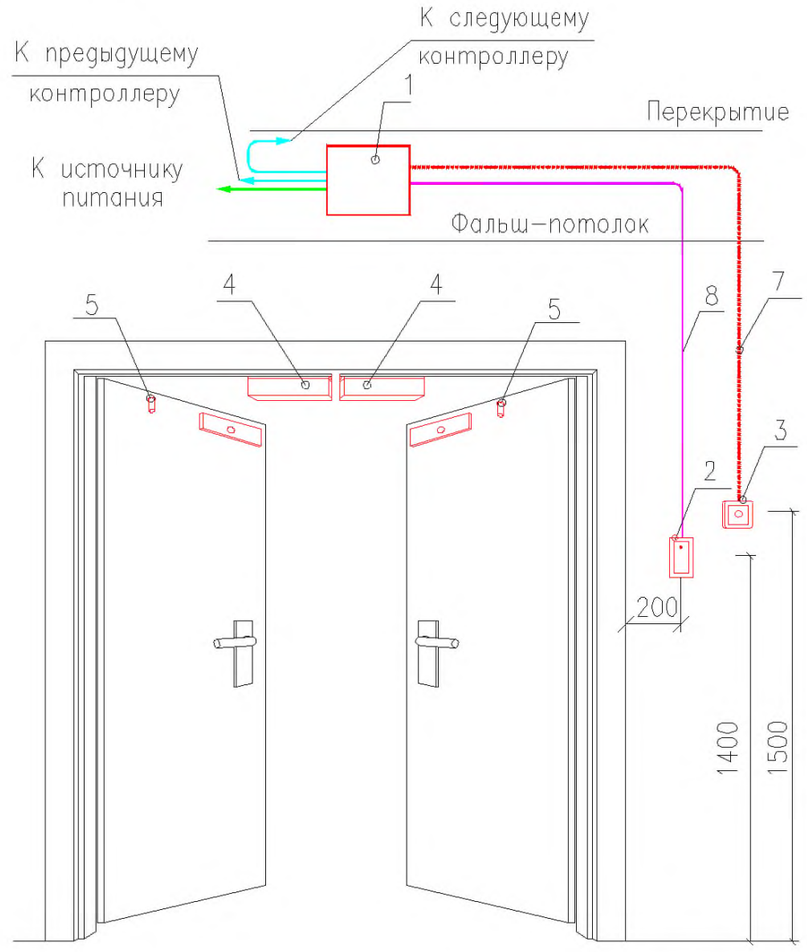
Вид со стороны защищаемого помещения

NN n/n	Наименование
1	Контроллер управления доступом
2	Бесконтактный считыватель с клавиатурой
3	Кнопка аварийной разблокировки электромагнитного замка
4	Электромагнитный замок
5	Извещатель охранный магнитоконтактный
6	Доводчик дверной
7	Провод
8	Провод

Схемы установки средств СКУД на двустворчатой двери



Вид со стороны коридора



Вид со стороны защищаемого помещения

NN n/n	Наименование	NN n/n	Наименование
1	Контроллер управления доступом	5	Извещатель охранный магнитоконтактный
2	Бесконтактный считыватель с клавиатурой	6	Доводчик дверной
3	Кнопка аварийной разблокировки электромагнитного замка	7	Провод
4	Электромагнитный замок	8	Провод

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к четвертой категории»

Москва 2016 г.

СОДЕРЖАНИЕ

№ раздела	Наименование системы	№ листов
1	Система охранно-тревожной сигнализации.	3-52
2	Система контроля и управления доступом.	53-78

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к четвертой категории»

Система охранно-тревожной сигнализации.

РАЗДЕЛ 1

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	6
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	8
3.	СИСТЕМА ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ (СОТС)	8
3.1	Назначение СОТС	8
3.2	Состав СОТС	9
3.3	Средства обнаружения проникновения	9
3.4	Критерии выбора СОТС	27
3.5	Организация передачи информации на пульт централизованного наблюдения (ПЦН)	27
3.6	Электропитание	28
3.7	Общие требования к минимально необходимому составу СОТС	30

ПРИЛОЖЕНИЯ

Приложение 1.	Условные обозначения.	35
Приложение 2.	Схема блокировки двери, окна извещателем охранным магнитоконтактным.	36
Приложение 3.	Схема установки извещателя охранного ударноконтактного для блокировки окна.	37
Приложение 4.	Схема установки извещателя охранного поверхностного звукового (акустического).	38
Приложение 5.	Схема установки извещателя охранного поверхностного оптико-электронного (инфракрасного).	39
Приложение 6.	Схема установки извещателя охранного объёмного ультразвукового.	40
Приложение 7.	Схема установки извещателя охранного объёмного радиоволнового.	41
Приложение 8.	Схема установки извещателя охранного объёмного оптико-электронного (инфракрасного).	42
Приложение 9.	Схема установки извещателя охранного поверхностного вибрационного на стене.	43
Приложение 10.	Схема установки извещателя охранного поверхностного вибрационного с датчиком наклона.	44
Приложение 11.	Схема установки извещателя охранного поверхностного вибрационного для охраны немонолитной (многосекционной) конструкции.	45
Приложение 12.	Схема установки извещателя охранного объёмного совмещённого (ИК+АК).	46

Приложение 13.	Схема установки извещателя охранного поверхностного совмещённого (ИК+АК).	47
Приложение 14.	Схема блокировки венткороба омическим извещателем.	48
Приложение 15.	Схема блокировки окна омическим извещателем.	49
Приложение 16.	План расположения оборудования СОТС в помещении ПЦО.	50
Приложение 17.	Схема структурная СОТС спецпомещения.	51
Приложение 18.	План расположения оборудования СОТС в помещении опорного пункта полиции.	52

1. ОБЩАЯ ЧАСТЬ

Методические рекомендации по оснащению ведомственных объектов СОТС разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 02.01.2013 № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;

- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- ГОСТ Р 50658-94 (МЭК 60839-2-4:1990) «Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений»;
- ГОСТ Р 50659-12 «Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний»;
- ГОСТ Р 50777-14 «Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок Общие технические требования и методы испытаний»;
- ГОСТ Р 51186-98 «Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний»;
- Р 78.36.018–2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- Р 78.36.019–2012 «Рекомендации по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий»;
- Р 78.36.028-2012 «Рекомендации. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов»;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану. Методические рекомендации»;
- Р 78.36.032-2013 «Инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1.»
- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения;

- Р 78.36.050-2015 «Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних периметров, дверей, окон, витрин и подступов к отдельным предметам»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА

В соответствии с пунктом 4.4 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом IV категории по степени потенциальной угрозы понимается обособленное помещение или группа помещений, расположенных в зданиях или сооружениях, не относящихся к системе органов внутренних дел Российской Федерации, в которых внутриобъектовый режим (ВР) не требует осуществления пропускного режима (ПР) и круглосуточного дежурства

3. СИСТЕМА ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ

3.1 Назначение системы охранно-тревожной сигнализации.

СОТС – это совокупность совместно действующих технических средств обнаружения проникновения (попытки проникновения) на охраняемый объект, сбора, обработки, передачи и представления в заданном виде информации о проникновении (попытке проникновения) и другой служебной информации.

При выборе технических средств охраны, для оборудования объекта СОТС рекомендуется применять приборы, указанные в «Списке технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (действующая редакция).

3.2 Состав СОТС.

СОТС включает в себя:

- средства обнаружения проникновения (охранные извещатели);
- средства тревожной сигнализации (СТС);
- приборы приемно-контрольные (ППК), и охранно-пожарные (ППКОП), устройство оконечное объектовое (УОО) системы передачи извещений (СПИ);
- средства оповещения (оповещатели световые, звуковые, комбинированные светозвуковые);
- СПИ на пульт централизованного наблюдения (ПЦН);
- источники вторичного электропитания (ИВЭП).

3.3 Средства обнаружения проникновения.

3.3.1 Классификация средств обнаружения проникновения.

Средства обнаружения (охранные извещатели), предназначенные для применения на объектах, классифицируют по следующим признакам функционального назначения.

3.3.1.1 По способу приведения в действие:

- автоматические;
- ручные (ножные).

3.3.1.2 По условиям эксплуатации:

- в отапливаемых помещениях;
- в помещениях с нерегулируемыми и неконтролируемыми параметрами температуры и влажности воздуха (в том числе под навесами);
- для эксплуатации на открытом воздухе.

3.3.1.3 По виду зоны, контролируемой автоматическим извещателем:

- точечные;
- линейные;
- поверхностные;
- объёмные.

3.3.1.4 По физическим принципам, положенным в основу обнаружения:

- электроконтактные;
- магнитоконтактные;
- ударноконтактные;
- ёмкостные;
- радиоволновые;
- оптико-электронные;
- вибрационные;
- звуковые (акустические).

3.3.1.5 По способу электропитания – на обеспечиваемые электропитанием от:

- источника постоянного тока;
- сети переменного тока;
- шлейфа сигнализации охранного приемно-контрольного прибора или оконечного объектового устройства системы передачи извещений;
- автономных источников.

3.3.1.6 По сочетанию принципов обнаружения:

- использующие один физический принцип;
- использующие два и более физических принципа: комбинированные, совмещенные.

3.3.2 Типы средств обнаружения, их назначение и функции.

Существует 12 типов средств обнаружения проникновений и угроз различных видов:

- магнитоконтактные извещатели для блокировки дверных, оконных конструкций и отдельных предметов;
- ударно-контактные извещатели для блокировки остеклённых конструкций;
- звуковые извещатели для блокировки остеклённых конструкций;
- вибрационные извещатели для блокировки строительных конструкций и сейфов;
- ультразвуковые извещатели для блокировки помещений и витрин;
- оптико-электронные пассивные извещатели для блокировки внутреннего пространства помещений;
- оптико-электронные активные извещатели для блокировки проёмов помещений и отдельных предметов;
- радиоволновые извещатели для блокировки внутреннего пространства помещений;
- ёмкостные извещатели для блокировки отдельных предметов;
- комбинированные извещатели для блокировки внутреннего пространства помещений;
- совмещённые извещатели для блокировки внутреннего пространства помещений и остеклённых конструкций;
- извещатели тревожной сигнализации о нападении (тревожные кнопки, педали).

3.3.2.1. Магнитоконтактные извещатели (Рисунок 1-4).

Магнитоконтактные извещатели применяют для блокировки «на открывание» подвижных строительных конструкций (дверей, окон, фрамуг, люков, ворот, т.п.), а также для блокировки «на перемещение» предметов (музейных или выставочных экспонатов, картин, товаров на витринах и стеллажах и т.п.).

Магнитоконтактные извещатели конструктивно состоят из двух частей: исполнительного блока (магнитоуправляемого датчика на основе геркона) и задающего блока, заключенного в отдельный корпус из «немагнитных» материалов (пластик, алюминий) управляющего элемента. В качестве

управляющего элемента используют постоянный магнит, фрагмент магнитопровода или магнитопровод самой защитной конструкции.

Исполнительный блок извещателя устанавливают на неподвижную часть охраняемой конструкции, задающий блок – на перемещаемую (открываемую, сдвигаемую, наклоняемую) часть охраняемой конструкции.



Рисунок 1. Магнитоконтактный извещатель для блокировки дверных, оконных конструкций и отдельных предметов.



Рисунок 2. Магнитоконтактный извещатель для открытого монтажа на конструкциях, выполненных из магнитных материалов.



Рисунок 3. Магнитоконтактный извещатель для скрытого монтажа на конструкциях, выполненных из немагнитных материалов.



Рисунок 4. Магнитоконтактный извещатель для скрытого монтажа на конструкциях, выполненных из магнитных материалов.

Сигнал «тревога» данные извещатели выдают посредством размыкания контактов встроенного геркона.

В зависимости от конструктивного исполнения магнитоконтактные извещатели подразделяют на датчики, предназначенные для открытой установки на поверхности охраняемой конструкции и датчики для скрытой установки в охраняемую конструкцию.

3.3.2.2 Концевые выключатели.

Концевые выключатели конструктивно состоят из одного блока, применяются для блокировки ворот, люков на открывание (Рисунок 5).



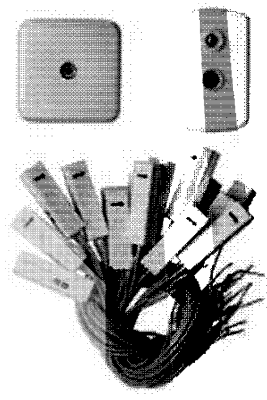
Рисунок 5. Концевой выключатель.

3.3.2.3 Ударно-контактные извещатели (Рисунок 6).

Ударно-контактные извещатели предназначены для использования в составе систем охранной сигнализации с целью обнаружения разрушения установленного в строительной конструкции стекла или стеклопакета при попытке нарушителя проникнуть в защищаемое помещение через эту остекленную конструкцию.

Ударно-контактные извещатели состоят из блока обработки сигналов (БОС) и комплекта миниатюрных датчиков разрушения стекла, устанавливаемых непосредственно на стекла, охраняемые извещателем.

В ударно-контактных извещателях срабатывание геркона происходит под воздействием вибрационных колебаний определенной амплитуды, длительности и направления распространения, возникающих при разрушении стекла.



\

Рисунок 6. Ударно-контактные извещатели для остеклённых конструкций.

3.3.2.4 Извещатели охранные поверхностные звуковые (акустические) для блокировки остеклённых конструкций (Рисунок 7).

Извещатели охранные поверхностные звуковые предназначены для обнаружения разрушения остеклённых конструкций в помещениях.

Дальность действия определяется расстоянием от извещателя до наиболее удалённой точки поверхности контролируемого стекла.

Минимальная охраняемая площадь представляет собой минимально допустимую для конкретного типа извещателя площадь поверхности охраняемого им стекла. Как правило, значение минимальной охраняемой площади устанавливают в диапазоне от 0,05 до 0,1 $м^2$.

Если в охраняемой конструкции установлены стёкла меньших размеров, то необходимо использовать извещатели другого принципа действия, например, ударно-контактные.



Рисунок 7. Извещатели охранные поверхностные звуковые (акустические) для блокировки остеклённых конструкций.

Не следует применять извещатели для блокировки стёкол, имеющих:

- толщину, не соответствующую диапазону, указанному в сопроводительной документации на извещатель;
- линейные размеры, не соответствующие требованиям к минимальной охраняемой площади, указанной в сопроводительной документации на извещатель;
- видимые повреждения (царапины, трещины, сколы и т.п.), снижающие прочность конструкции;
- некачественное (слабое, неплотное, ненадёжное) закрепление стекла в строительной конструкции (раме).

Для обеспечения надёжного обнаружения необходимо при установке извещателя ориентировать его зону обнаружения на блокируемые стёкла.

Для исключения ложных срабатываний от акустических помех извещатель не рекомендуется устанавливать в помещениях:

- с высоким уровнем звуковых шумов (более 65 дБ, что ориентировочно соответствует громкому разговору двух людей в помещении на удалении 3–4 м от извещателя);
- с плохой звукоизоляцией.

В помещении, на период его охраны, должны быть закрыты двери, форточки, отключены вентиляторы, радиоприёмники (или трансляционные громкоговорители) и другие возможные источники звуковых помех.

3.3.2.5 Вибрационные извещатели для блокировки строительных конструкций и сейфов (Рисунок 8).

Вибрационные извещатели предназначены для обнаружения на ранней стадии попытки умышленного разрушения, повреждения или взлома различных строительных конструкций (стены, перекрытия, двери и т.д.), металлических сейфов (шкафов).

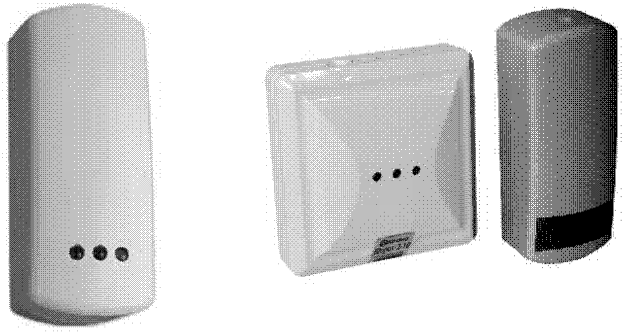


Рисунок 8. Вибрационные извещатели для блокировки строительных конструкций и сейфов (металлических шкафов).

Принцип действия вибрационных извещателей основан на анализе вибрационных сигналов, возникающих в строительных конструкциях при нанесении разрушающих воздействий с целью проникновения в охраняемое помещение.

С помощью таких извещателей можно защитить от вандализма лицевые панели банкоматов, организовать охрану конструкций, выполненных с применением многослойных защитных стёкол и стеклоблоков, кирпичных стен и перегородок, стальных решёток, деревянных дверей, оконных рам (при небольшом размере многосекционных остеклённых проёмов), перекрытий, конструкций из фанеры и древесностружечных плит.

Зона обнаружения вибрационного извещателя может охватывать смежные части сооружения, например, часть пола, потолка, примыкающей стены или капитальной перегородки, если угловое соединение жёстко состыковано. В этих случаях дальность действия извещателя для смежных конструкций уменьшается приблизительно на 25 % от установленного значения (новое значение радиуса действия определяется опытным путём).

Охрана строительной конструкции может производиться посредством установки на ней одного или нескольких однопозиционных извещателей или нескольких датчиков вибрации многопозиционного извещателя.

Для охраны небольших конструкций, а также дверей, шкафов, сейфов или банкоматов, если их количество не превышает трёх, рекомендуется использовать однопозиционные извещатели, для охраны больших помещений или большого числа строительных конструкций – многопозиционные.

Извещатели обнаруживают разрушающие воздействия на охраняемые конструкции, производимые средствами взлома различной производительности и физического принципа действия, такими, как:

– ручные режущие инструменты (ручные дрели, пилы, напильники);

- термические режущие инструменты (газорежущее, электродуговое оборудование);
- электрические неударные инструменты (электродрели, дисковые пилы типа «болгарка»);
- электрические вращательные инструменты с ударом (электродрели с перфорацией, перфораторы);
- ручные ударные инструменты (молотки, кувалды, ломы, колуны, кирки);
- электрические ударные инструменты (отбойные молотки).

3.3.2.6 Ультразвуковые извещатели для блокировки объёма помещений (Рисунок 8, 9).

Ультразвуковой извещатель использует принцип активной локации.

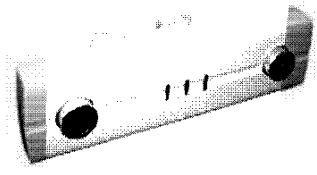


Рисунок 9. Ультразвуковой извещатель для блокировки внутреннего пространства помещения объемом 250 м^3.

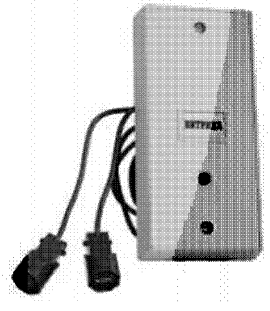


Рисунок 10. Ультразвуковой извещатель для блокировки внутреннего пространства витрин, экспозиций и небольших хранилищ ценностей объёмом от 0,03 до 1,00 м^3.

Ультразвуковой извещатель для блокировки внутреннего пространства помещения предназначен для обнаружения движения нарушителя или выявления открытого очага пламени в охраняемой зоне.

При выборе данного извещателя для охраны того или иного объекта необходимо иметь в виду, что акустические волны ультразвукового

диапазона, создаваемые извещателем, обладают способностью отражаться от любых твёрдых поверхностей, а также огибать препятствия сравнительно небольших размеров.

Поэтому есть возможность минимизировать образование так называемых «мёртвых зон» (зон нечувствительности).

На функционирование извещателя практически не влияют звуковые помехи, возникающие снаружи охраняемого помещения.

Перемещение мелких домашних животных (грызунов) в зоне обнаружения не вызывает ложных срабатываний извещателя, так как отражающая поверхность этих «нарушителей» (с учётом их малых размеров и наличия шерсти, поглощающей ультразвук) является пренебрежительно малой для извещателя.

Ультразвуковой извещатель для блокировки внутреннего пространства витрин, экспозиций и небольших хранилищ ценностей предназначен для обнаружения проникновения (попытки проникновения) в охраняемую витрину (объём), перемещения предметов в охраняемом объёме.

Извещатель обеспечивает контроль всего объёма охраняемой конструкции путем создания стационарного акустического поля.

3.3.2.7 Оптико-электронные пассивные инфракрасные (ИК) извещатели для блокировки внутреннего пространства помещений и проёмов в строительных конструкциях (Рисунок 11).

Оптико-электронные пассивные ИК извещатели разделяются по типу формируемой зоны обнаружения (ЗО):

- объёмные;
- поверхностные;
- линейные.



Рисунок 11. Извещатели оптико-электронные пассивные ИК.

Они предназначены для обнаружения нарушителя, перемещающегося или пересекающего ЗО.

Извещатели, формирующие объёмную ЗО, в свою очередь, подразделяются по способу установки (на стене или на потолке).

Пассивные оптико-электронные ИК извещатели имеют одноблочную конструкцию.

Принцип действия пассивных оптико-электронных ИК извещателей основан на регистрации изменения уровня теплового излучения.

Извещатель рекомендуется устанавливать таким образом, чтобы в его ЗО не попадали потоки тёплого воздуха. В период охраны в помещении должны быть закрыты окна (форточки, фрамуги), балконные и входные двери, отключены обогревательные вентиляторы, кондиционеры и т.п.

Если температура окружающего воздуха ниже (при установке в неотапливаемых помещениях) или выше допустимых значений рабочей температуры извещателя, то извещатель может не обнаруживать нарушителя.

Наличие на входном окне извещателя постоянной или переменной высокой освещённости, фактическое значение которой превышает 6500 лк (ГОСТ Р 50777-95 «Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 6. Пассивные оптико-электронные инфракрасные извещатели для закрытых помещений»), может являться причиной ложных срабатываний или пропуска нарушителя.

Причиной высокой освещённости может быть как солнце, так и источники искусственного освещения.

Для исключения влияния данного фактора на работу извещателя он должен быть установлен таким образом, чтобы на его входное окно не попадали прямые солнечные лучи и излучение от мощных осветительных приборов.

Следует иметь в виду, что резкое чередование на входном окне извещателя света и тени (вызванное, к примеру, перемещающимися по небу облаками, качающимися ветвями деревьев, перекрывающими солнце и т.п.) негативно влияет на работу извещателя и может являться причиной ложных срабатываний. При этом следует отметить, что сами качающиеся за окном ветки влияния на работоспособность пассивного ИК извещателя, установленного в помещении (при условии, что окна помещения закрыты, что обычно оговаривается в прилагаемой к извещателю эксплуатационной документации), не оказывают.

Оседание на входном окне извещателя твердых мелкодисперсных частиц приводит к уменьшению максимальной рабочей дальности действия и обнаружительной способности извещателя.

При наличие в ЗО крупногабаритных предметов и конструкций (сплошные, сетчатые, стеклянные перегородки), перемещение нарушителя за ними обнаружено не будет.

При этом обеспечить полное отсутствие таких предметов на большинстве объектов невозможно. В этом случае для обеспечения надёжной охраны необходимо установить несколько извещателей таким образом, чтобы все возможные пути перемещения нарушителя попадали в их ЗО.

Наличие на охраняемом объекте животных, перемещающихся в ЗО извещателя, может привести к ложному извещению о тревоге.

Для охраны таких объектов необходимо применять специальные извещатели, обладающие устойчивостью к перемещению в ЗО животных, а при выборе места их установки и монтаже строго выполнять требования, изложенные в прилагаемой к извещателям эксплуатационной документации.

3.3.2.8 Оптико-электронные активные ИК извещатели для блокировки периметров, конструкций, помещений и отдельных предметов (Рисунок 12, 13).

Линейные оптико-электронные извещатели (активные ИК извещатели) предназначены для обнаружения попыток проникновения на охраняемый объект и формирования извещения о тревоге. В отличие от пассивных ИК извещателей, регистрирующих тепловое излучение нарушителя, активные ИК извещатели регистрируют изменение собственного излучения, вызванное вторжением нарушителя в ЗО.

Достоинством активных ИК извещателей является то, что их обнаружительная способность не зависит от характеристик теплового излучения человека (нарушителя). Также они нечувствительны к изменению характеристик теплового излучения окружающих объектов (фона) и возникающим тепловым помехам.

К недостаткам активных ИК извещателей можно отнести то, что они способны формировать только линейную ЗО, что ограничивает их область применения. Отчасти эта проблема может быть решена путём организации поверхностной ЗО (так называемого ИК барьера) за счет применения извещателей, формирующих несколько ИК лучей, или построения ИК барьера из нескольких извещателей. Но при этом размеры ЗО для первого варианта будут небольшими, а второй вариант потребует увеличения финансовых затрат. К недостаткам можно отнести и их чувствительность к оптическим засветкам.

Активные ИК извещатели, как правило, имеют двухблочную конструкцию (Рисунок 12) и состоят из блока излучателя (БИ) и блока фотоприёмника (БФ), образующих оптическую систему.

Появление в ЗО извещателя оптически непрозрачного объекта вызывает прерывание (или снижение мощности) ИК луча, попадающего в приёмник, который анализирует величину и длительность этого прерывания в соответствии с заданным алгоритмом, формирует извещение о тревоге путём изменения сопротивления контактов, подключаемых к шлейфу сигнализации.



Рисунок 12. Активные линейные двухблочные ИК извещатели.

Также встречаются извещатели, имеющие одноблочную конструкцию (Рисунок 13), оптическая система которых состоит из излучателя и фотоприёмника, объединённых в одном корпусе, и светоотражателя (катафота).



Рисунок 13. Активный линейный одноблочный (с катафотом) ИК извещатель.

Активными ИК извещателями удобно блокировать проёмы ворот, имеющихся в здании (например, ворота боксов или гаражей для хранения

автотранспорта). Помимо прохода человека через проём, извещатель будет обнаруживать и проезд транспортного средства. Если ворота имеют распашную конструкцию и их створки открываются наружу, извещатель также будет обнаруживать факт открытия ворот.

Блокировка окон, световых фонарей и т.п. извещателями, установленными снаружи здания, применяется как для обнаружения проникновения в здание через проём, так и для обнаружения попыток несанкционированного воздействия на оконные конструкции (нередки случаи попыток проникновения в здание через оконный проём путём вынимания стекла без его разрушения, при котором акустические извещатели, установленные в здании, извещение о тревоге не формируют).



Рисунок 14. Радиоволновые извещатели для блокировки внутреннего пространства закрытых помещений.

3.3.2.9 Радиоволновые извещатели для блокировки внутреннего пространства закрытых помещений (Рисунок 14).

В основе принципа действия радиоволновых извещателей лежит эффект Доплера. При отражении сверхвысокочастотного (СВЧ) радиосигнала от движущегося объекта его частота изменяется.

По конструкции извещатели, как правило, имеют одноблочную схему, в которой содержатся два основных узла: СВЧ модуль, который излучает и принимает сверхвысокочастотные колебания, и процессор, который по определённому алгоритму анализирует параметры доплеровского сигнала, поступающего со смесителя, и принимает решение о формировании извещения о тревоге.

При работе извещателя создаётся объёмная зона обнаружения. Электромагнитное излучение распространяется в объёме помещения и ограничивается его капитальными конструкциями.

Вместе с тем, излучение может проникать в соседнее помещение через перегородки, изготовленные на основе древесностружечных плит, фанеры, гипсокартона и т.д., через деревянные и пластмассовые двери, на улицу – через оконные проёмы. В этом случае движение людей, крупных животных, автомобилей за габаритами помещения может привести к формированию ложного сигнала тревоги.

Радиоволновые извещатели, предназначенные для блокировки внутреннего пространства помещений, сохраняют работоспособность в

широком диапазоне температур, не реагируют на световые засветки, тепловые потоки и сквозняки, имеют стабильную объёмную зону обнаружения, допускают маскировку радиопрозрачными материалами.

Извещатели могут формировать ложные сигналы тревоги от вибрации крупных предметов, люминесцентного освещения, перемещения людей или механизмов за оконными проёмами или тонкими перегородками.

3.3.2.10 Комбинированные извещатели для блокировки внутреннего пространства помещений (Рисунок 15, 16).



Рисунок 15. Комбинированный (СВЧ + ИК) извещатель для блокировки внутреннего пространства помещения (устанавливается на стене).



Рисунок 16. Комбинированный (СВЧ + ИК) извещатель для блокировки внутреннего пространства помещения (устанавливается на потолке).

Рекомендуемая область применения комбинированных (СВЧ + ИК) извещателей – блокировка помещений с повышенным уровнем помех, мест сосредоточения ценностей, музейных экспонатов, оргтехники, а также помещений критически важных объектов.

В извещателях этого класса используются два физических принципа обнаружения движущегося объекта: регистрация изменения теплового фона, возникающего при пересечении чувствительных зон, формируемых

оптической системой, и регистрация наличия доплеровской составляющей в спектре отражённого сигнала, создаваемого СВЧ модулем. При появлении нарушителя в зоне обнаружения срабатывают оба канала (в любой последовательности, с разнесением по времени), формируя извещение о тревоге.

Комбинированные извещатели обладают повышенной помехоустойчивостью по сравнению с собственно радиоволновыми или пассивными ИК извещателями, так как вероятность возникновения в помещении помех, одновременно воздействующих на два канала, достаточно мала.

Комбинированные (СВЧ + ИК) извещатели надёжно работают в помещениях с повышенным уровнем помех, в которых радиоволновые или оптико-электронные пассивные извещатели, функционирующие по отдельности, выдают ложные извещения о тревоге.

3.3.2.11 Комбинированные (ультразвуковые + ИК) извещатели для блокировки внутреннего пространства помещений (Рисунок 17).

Основная область применения комбинированных (ультразвуковых + ИК) извещателей – помещения, имеющие следующие особенности:

- со сложной помеховой обстановкой внутри и снаружи помещения;
- с остеклёнными (оконными, дверными) конструкциями, выходящими на оживлённую улицу, в том числе остеклённые вестибюли зданий, бизнес-центров, магазинов, выставочных павильонов;

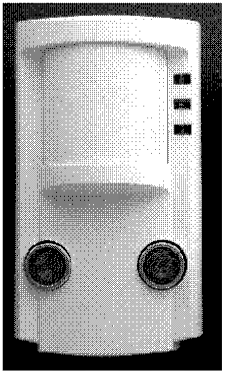


Рисунок 17. Комбинированный (ультразвуковой + ИК) извещатель для блокировки внутреннего пространства помещений.

- имеющие некапитальные стены или перегородки со смежными помещениями, где возможно нахождение людей в период охраны.

Принцип работы комбинированных (ультразвуковых + ИК) извещателей заключается в комбинировании двух принципов обнаружения стандартной цели (человека) в охраняемом помещении.

Первый принцип заключается в регистрации ИК излучения при пересечении человеком элементарных зон обнаружения, формируемых оптической системой ИК канала извещателя. Это объясняется тем, что температура человека отличается от температуры предметов в помещении.

Разница температур является критерием обнаружения нарушителя в охраняемом помещении.

Второй принцип работы извещателя основан на эффекте Доплера, в соответствии с которым частота ультразвукового сигнала, отражённого от движущегося препятствия, отличается от первоначальной на величину, которая прямо пропорциональна излучаемой частоте и радиальной скорости движения отражателя и обратно пропорциональна скорости распространения ультразвука в контролируемой среде.

Основу ультразвукового канала, как правило, составляют два пьезоэлектрических преобразователя (приёмник и передатчик), работающих на несущей частоте за пределами слышимости, формирующих в окружающем пространстве объёмную зону обнаружения.

Следует отметить, что размеры зоны можно изменять так, как требуется в конкретных условиях (габаритах помещения), в том числе для создания локального охраняемого пространства.

3.3.2.12 Совмещённые извещатели для блокировки внутреннего пространства помещений и остеклённых конструкций (Рисунок 18).

Область применения совмещённых (ИК + акустический) извещателей – помещения с остеклёнными (оконными, дверными) конструкциями.



Рисунок 18. Совмещённые извещатели для блокировки внутреннего пространства помещений и остеклённых конструкций.

Извещатели сочетают в себе два принципа обнаружения (ИК + акустический), обнаруживают движение нарушителя в закрытом охраняемом помещении и разрушение строительных конструкций, выполненных с использованием листового стекла (обычного, армированного, узорчатого, закалённого, трёхслойного, ударостойкого), стеклоблоков, однокамерных и двухкамерных стеклопакетов.

При появлении человека в зоне обнаружения срабатывает ИК канал обнаружения, при разбитии стекла – акустический канал (в любой

последовательности или одновременно). При этом выдаётся извещение о тревоге путем размыкания контактов соответствующего выходного реле.

Акустический канал извещателя предназначен для блокировки остеклённых конструкций (окон, витрин, витражей и т.п.) на разбитие.

Принцип действия инфракрасного канала извещателя основан на регистрации разницы между интенсивностью инфракрасного излучения, исходящего от тела человека, и фоновой температурой окружающей среды.

Расстояние от извещателя до самой удалённой точки охраняемой стеклянной поверхности не должно превышать 6м.

Не следует применять совмещённые (ИК+акустический) извещатели в помещении со стёклами, имеющими:

- толщину, не соответствующую диапазону, указанному в сопроводительной документации на извещатель;
- линейные размеры, не соответствующие требованиям к минимальной охраняемой площади, указанной в сопроводительной документации на извещатель;
- видимые повреждения (царапины, трещины, сколы и т.п.), снижающие прочность конструкции;
- плохое (слабое, неплотное, ненадёжное) закрепление стекла в строительной конструкции (раме).

Параметры помехозащищённости определяют условия для устойчивой работы извещателя без выдачи ложных сигналов тревоги. Для этого в охраняемом помещении должны быть выполнены определённые требования по исключению воздействия опасных помех акустического и электромагнитного характера.

Для исключения ложных срабатываний от акустических помех извещатель не рекомендуется устанавливать в помещениях:

- с высоким уровнем звуковых шумов (более 65 дБ, что ориентировочно соответствует громкому разговору двух людей в помещении на удалении 3–4 м от извещателя);
- с плохой звукоизоляцией.

В помещении на период его охраны должны быть закрыты двери, окна, фрамуги, форточки, отключены вентиляторы, радиоприёмники (трансляционные громкоговорители) и другие возможные источники звуковых помех.

Следует иметь в виду, что наличие вибрации стен в месте размещения извещателя может привести к формированию на выходе его чувствительного элемента переменного электрического сигнала, приводящего к снижению чувствительности или к появлению ложных сигналов тревоги.

При выборе места установки извещателя на охраняемом объекте необходимо также учесть следующие требования по ИК каналу:

а) не рекомендуется устанавливать извещатель в непосредственной близости от вентиляционных отверстий, окон и дверей, у которых создаются

воздушные потоки, а также рядом с радиаторами центрального отопления, другими отопительными приборами и источниками тепловых помех;

б) нежелательно прямое попадание на входное окно извещателя светового излучения от ламп накаливания, автомобильных фар, солнца;

в) не рекомендуется нахождение в зоне обнаружения каких-либо перегородок, крупногабаритных предметов мебели и т.п., создающих «мёртвые зоны», в которых перемещение человека не обнаруживается.

3.3.2.13 Извещатели для тревожной сигнализации (ТС) о нападении (тревожные кнопки, педали и т.п.) (Рисунок 19).

Для оперативной передачи сообщений в дежурные части органов внутренних дел или на ПЦН о нападении нарушителя объект оборудуют техническими средствами ТС.



Рисунок 19. Тревожная кнопка с фиксацией.

Извещатель (Рисунок 19) представляет собой тревожную кнопку для выдачи извещения о нападении с фиксацией извещения. Перевод извещателя в дежурный режим после нажатия кнопки осуществляется при помощи ключа, который хранится в подразделении охраны.



Рисунок 20. Тревожный извещатель для подачи сигнала тревоги ногой при нападении преступников.

Извещатель (Рисунок 20) предназначен для включения средств сигнализации ногой при нападении преступников на сотрудников.

Система ТС должна быть выполнена «без права отключения», выведена на пульт внутренней охраны, на ПЦН.

3.4 Критерии выбора СОТС.

Критерии выбора СОТС:

- назначение и функции, выполняемые техническими средствами охранной сигнализации;
- вид предполагаемой угрозы объекту;
- помехозащищённость;
- надёжность;
- круглосуточный режим функционирования;
- функционирование в автоматическом режиме;
- функционирование в автономном режиме;
- самодиагностирование;
- бесперебойное электропитание;
- возможность расширения как функциональных, так и количественных характеристик системы;
- интеграция в единую систему безопасности;
- защита информации от несанкционированного внешнего доступа и копирования при передаче от периферийных узлов на пульт дежурного;
- соответствие российским и международным стандартам.

3.5 Организация передачи информации на пульт централизованного наблюдения (ПЦН).

3.5.1 Передача извещений о срабатывании охранной сигнализации (ОС) с объекта на ПЦН может осуществляться с ППК малой ёмкости, внутреннего пульта охраны или УОО СПИ.

3.5.2 Количество рубежей ОС, выводимых на ПЦН отдельными условными номерами, определяется совместным решением руководителя объекта и подразделения вневедомственной охраны исходя из категории объекта, анализа риска и потенциальных угроз объекту, возможностей интеграции и документирования ППК (внутренним пультом охраны или УОО СПИ) поступающей информации.

3.5.3 Рубежи ОС должны выводиться на ПЦН с пульта внутренней охраны, ППК или УОО СПИ, обеспечивающих запоминание тревожного состояния и его фиксацию на выносном световом (звуковом) оповещателе или индикаторе.

Извещения от шлейфов ОС одним объединенным сигналом выводятся на ПЦН.

3.5.4 Для исключения доступа посторонних лиц к извещателям, ППК, разветвительным коробкам, другой установленной на объекте аппаратуре охраны должны приниматься меры по их маскировке и скрытой установке. Крышки клеммных колодок данных устройств должны быть опломбированы (опечатаны) электромонтёром охранно-пожарной сигнализации или

инженерно-техническим работником подразделения вневедомственной охраны с указанием фамилии и даты в технической документации объекта.

3.5.5 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 ПЦН в составе ТС.

3.5.6 Извещения ОС и ТС могут передаваться на ПЦН 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 с обязательным контролем канала между охраняемым объектом и ПЦН.

Проводная среда передачи информации реализуется в виде:

- абонентской телефонной сети общего пользования или специально прокладываемой выделенной линии оператора связи (технология DSL, FTTC, FTTB, в т.ч. по технологии GPON);
- линии связи интернет провайдеров (коаксиальный кабель, «витая пара», оптоволоконный кабель);

Беспроводная среда передачи информации может быть реализована в виде:

- выделенных рабочих частот УКВ радиодиапазона;
- защищённых каналов передачи данных сетей сотовых операторов стандарта GSM(GPRS) - VPN.

3.6 Электропитание.

СОТС, согласно Р 78.36.032-2013 (п.9) и ПУЭ (п.1.2.17.), относится к 1 категории электроприёмников по надёжности электроснабжения, в силу чего 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 электропитание от аккумуляторных батарей).

При пропадании основного электропитания 220В, 50 Гц СОТС автоматически переходит на электропитание от резервного источника электропитания (аккумулятора) постоянного напряжения 12В без выдачи сигналов тревоги, но с формированием служебного сообщения «переход на резервное электропитание».

При переходе на электропитание от резервного источника электропитания (аккумулятора) должна обеспечиваться бесперебойная работа оборудования и извещателей СОТС не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги.

Допускается уменьшать время работы от резервного источника электропитания при наличии автоматического или иного оповещения

подразделения вневедомственной охраны о моменте отключения основного электропитания:

- в городах и поселках городского типа - до 4 часов в дежурном режиме и до 1 часа в режиме тревоги;
- 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.

Пример расчёта резервного источника электропитания.

№	Наименование	Кол-во, шт.	Ток потребления одним устройством в дежурном режиме, мА	Ток потребления одним устройством в режиме тревоги, мА	Суммарный ток потребления в дежурном режиме, мА	Суммарный ток потребления, в режиме тревоги, мА
1	Устройство взятия-снятия СПИ	1	20	20	20	20
2	Устройство оконечное объектовое СПИ	1	150	250	150	250
3	Извещатель охранный объёмный оптико-электронный	1	20	20	20	20
4	Извещатель охранный поверхностный оптико-электронный	1	20	20	20	20
5	Извещатель охранный поверхностный звуковой	1	20	20	20	20
6	Извещатель охранный совмещенный с датчиком наклона	1	25	25	25	25
7	Оповещатель охранно-пожарный световой	1	20	20	20	20
8	Оповещатель охранно-пожарный звуковой	1	0	60	0	60
	ИТОГО				275	435

Необходимая ёмкость аккумулятора рассчитывается по формуле:
$Q(мАч) = 1,2 \times Iр(мА) \times t(ч)$,

где:

1,2 - коэффициент запаса ёмкости;

Ip - потребляемый ток (мА);

t - требуемое время работы (ч).

Необходимая ёмкость аккумулятора в дежурном режиме составляет:

1,2 х 275 мА х 4 ч =1320 мАч.

Необходимая ёмкость аккумулятора в режиме тревоги составляет:

1,2 х 435 мА х 1 ч = 522 мАч.

1320 мАч + 522 мАч = 1842 мАч.

Согласно расчётам выбираем резервированный источник электропитания, удовлетворяющий следующим характеристикам:

- максимальный ток нагрузки не менее 0,435 А;
- ёмкость аккумулятора должна быть не менее 1,842 Ач.

Заземление оборудования и устройств должно выполняться в соответствии с требованиями СНиП 3.05.06-85, ПУЭ, технической документации предприятий-изготовителей.

3.7 Общие требования к минимально необходимому составу СОТС.

3.7.1 Требования к защите СОТС зданий, помещений, отдельных предметов.

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

Для защиты вентиляционных шахт, коробов и дымоходов диаметром более 200 мм, имеющих выход за границы охраняемой территории объекта, в том числе на крыши зданий, а также в смежные неохраняемые помещения и своим сечением входящие в охраняемые помещения, допускается использование фальшрешёток с ячейкой 100 х 100 мм, выполненных из металлических трубок с диаметром отверстия не менее 6 мм для протяжки провода шлейфа сигнализации «на обрыв», а также применение иных ТСО.

Ключи от замков на оконных решётках и дверях запасных выходов должны быть размещены в непосредственной близости или в специально выделенном помещении (в помещении охраны) в ящике, шкафу или нише, заблокированных ОС.

Устанавливаемые в зданиях СОТС должны вписываться в интерьер помещения и по возможности устанавливаться скрыто.

В разных рубежах необходимо применять охранные извещатели, работающие на различных физических принципах действия.

Количество шлейфов ОС должно определяться тактикой охраны, размерами зданий, строений, сооружений, этажностью, количеством уязвимых мест, а также точностью определения места проникновения для быстрого реагирования на извещения о тревоге.

Периметр охраняемого здания (помещений), как правило, следует разделять на охраняемые зоны (фасад, тыл, боковые стороны здания (помещений), центральный вход и другие участки) с выделением их в самостоятельные шлейфы сигнализации и выдачей раздельных сигналов на ППК.

Для усиления охраны и повышения её надежности на объектах следует устанавливать дополнительные извещатели-ловушки. Сигналы ловушек выводятся по самостоятельным или, при отсутствии технической возможности, по имеющимся шлейфам ОС.

Помещения объектов оборудуются многорубежной системой ОС, а вспомогательные помещения – однорубежной.

3.7.2 Охранная сигнализация.

ОС оборудуются:

- периметр зданий (помещений) и сооружений (оконные проемы, двери, люки, ворота и другие) с выводом на ПЦН;
- отдельные служебные помещения с выводом на ПЦН;
- специальные помещения с выводом на ПЦН.

Первым рубежом ОС, в зависимости от вида предполагаемых угроз объекту, блокируют:

- входные двери, погрузочно-разгрузочные люки, ворота – на «открывание», «разрушение» и «пролом»;
- деревянные, стеклянные и остеклённые конструкции – на «открывание», «разрушение» и «разбитие» стекла;
- стены, перекрытия и перегородки, за которыми размещаются помещения других собственников – на «разрушение» и «пролом»;
- вентиляционные короба, дымоходы, места ввода/вывода коммуникаций сечением более 200 х 200 мм – на «разрушение» и «пролом».

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

Вторым рубежом ОС защищаются объемы помещений на «проникновение» с помощью объёмных извещателей различного принципа действия.

Третьим рубежом ОС в помещениях блокируются отдельные предметы, сейфы, металлические шкафы, в которых сосредоточены документы и ценности.

Специальные помещения: для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, архивы, хранилища, кассы и другие защищаются в два рубежа охраны.

Первым рубежом ОС блокируются:

1. Входные двери в помещения – на открывание;

2. Окна – на открывание и разбитие.

Вторым рубежом ОС – объём помещения.

Дополнительным рубежом ОС в помещениях могут блокироваться отдельные предметы, сейфы, металлические шкафы, в которых сосредоточены документы и ценности.

Для блокировки помещений двумя (тремя) рубежами охраны применяются охранные извещатели, работающие на различных физических принципах действия.

Сигнализация из специальных помещений должна быть выведена на ПЦН ближайшего подразделения вневедомственной охраны.

3.7.3 Тревожная сигнализация.

Для передачи тревожных извещений на ПЦН о противоправных действиях в отношении сотрудников и работников (угроз террористического и криминального характера) объект оборудуется устройствами ТС.

Кнопки тревожной сигнализации (КТС) на объекте должны устанавливаться:

- в специальных помещениях (хранения специальных средств, для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, архивах, хранилищах, кассах и других);
- в иных местах, регламентированных правовыми актами МВД России.

КТС размещаются в местах, по возможности незаметных для посетителей.

Решение о необходимости вывода сигнала на ПЦН принимается руководителем подразделения, в ведении которого находится объект, исходя из его функционального назначения, степени потенциальной опасности, которой он может подвергаться, а также анализа вероятных угроз объекту и характеристики его уязвимости.

Обобщённый сигнал от КТС подключается на ПЦН без права отключения.

Примечания:

1. Аттестованные помещения, а также помещения, предназначенные для обработки сведений, составляющих государственную тайну, оборудуются техническими средствами ОС, прошедшими сертификацию по стандартам ФСТЭК России и ФСБ России.

2. В случае отсутствия (с учетом объективных факторов) на объекте необходимых средств инженерно-технической укреплённости (решётки на окнах и т.д.) либо оснащённости объекта средствами инженерно-технической укреплённости более низкого класса защиты, рекомендуется оборудовать объект дополнительными рубежами охраны с использованием средств охранной сигнализации и системы охранной телевизионной.

Организация дополнительных рубежей охраны должна быть согласована с подразделением охраны и руководством объекта.

ПРИЛОЖЕНИЯ

Приложение 1

Условные обозначения

Наименование	Обозначение
Пульт управления программируемый	
Прибор приемно-контрольный охранно-пожарный	
Устройство взятия-снятия СПИ	
Устройство оконечное объектовое СПИ	
Релейный блок	
Извещатель охранный магнитоконтактный для деревянных окон, дверей	
Извещатель охранный магнитоконтактный для металлических дверей	
Извещатель охранный поверхностный оптико-электронный (пассивный ИК)	
Извещатель охранный объемный оптико-электронный (пассивный ИК)	
Извещатель охранный объемный радиоволновый	
Извещатель охранный совмещенный вибрационный с датчиком наклона.	
Извещатель охранный поверхностный звуковой (акустический)	
Кнопка тревожной сигнализации	
Оповещатель охранно-пожарный световой	
Оповещатель охранно-пожарный звуковой	
Источник резервированного электропитания 12В	
Шлейф сигнализации	

Приложение 2

Схема блокировки двери, окна извещателем охранным магнитоконтактным

Схема блокировки двери

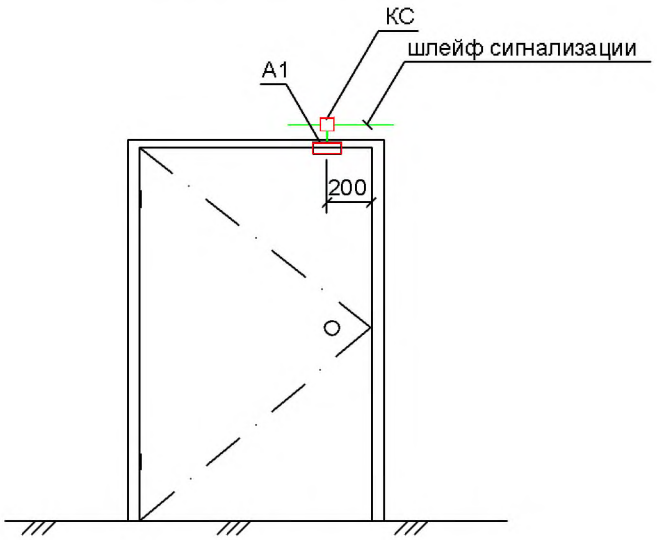
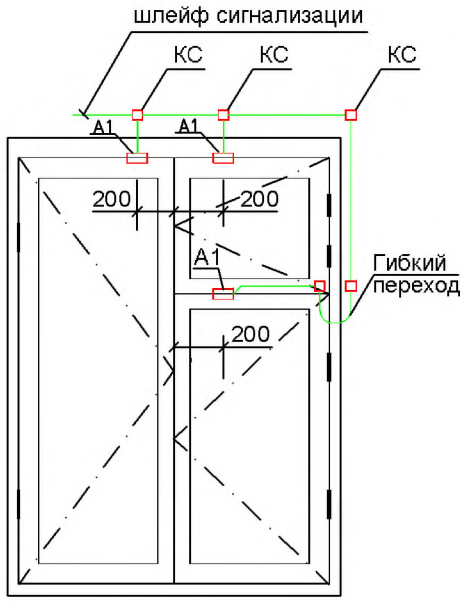


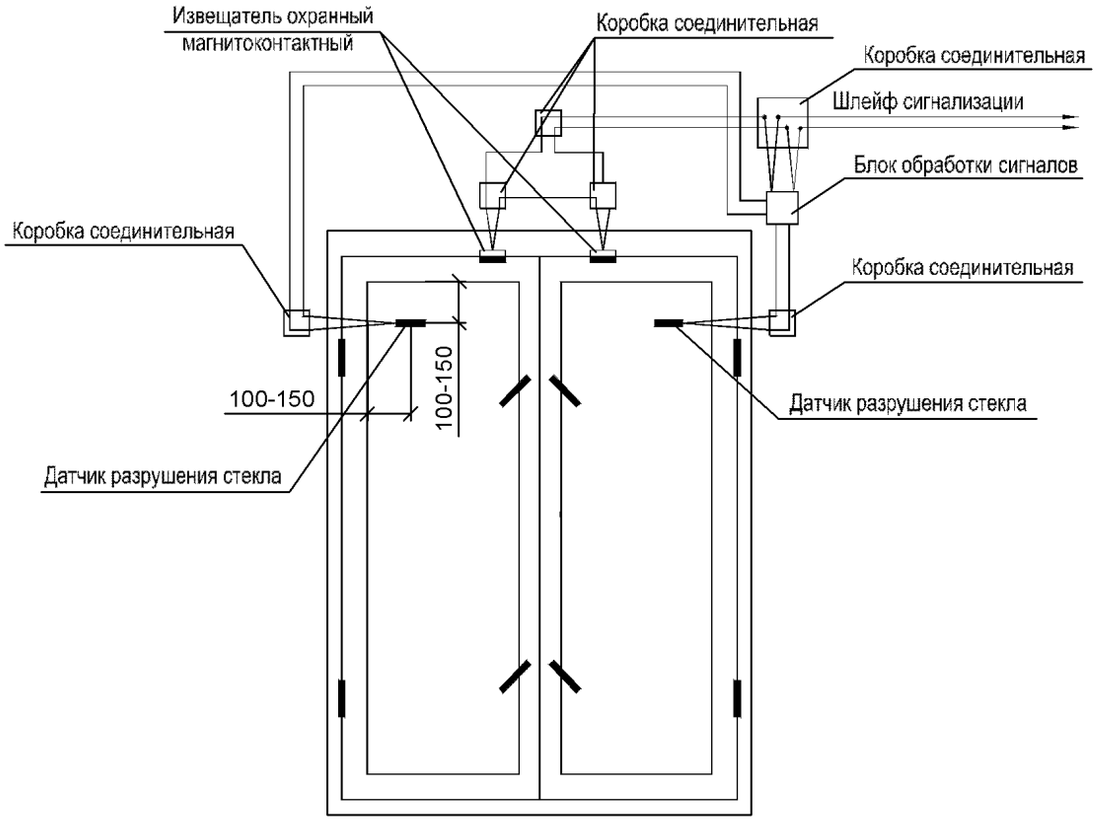
Схема блокировки окна



А1- Извещатель охранный магнитоконтактный
КС- Коробка соединительная

Приложение 3

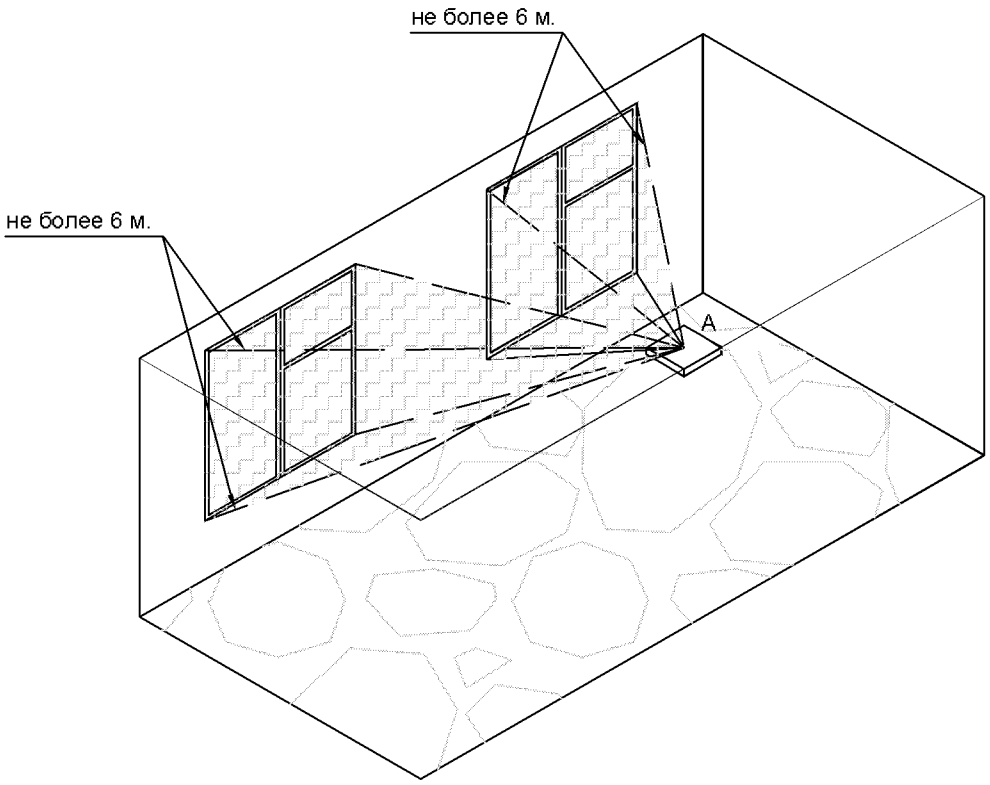
Схема установки извещателя охранного ударно-контактного для блокировки окна



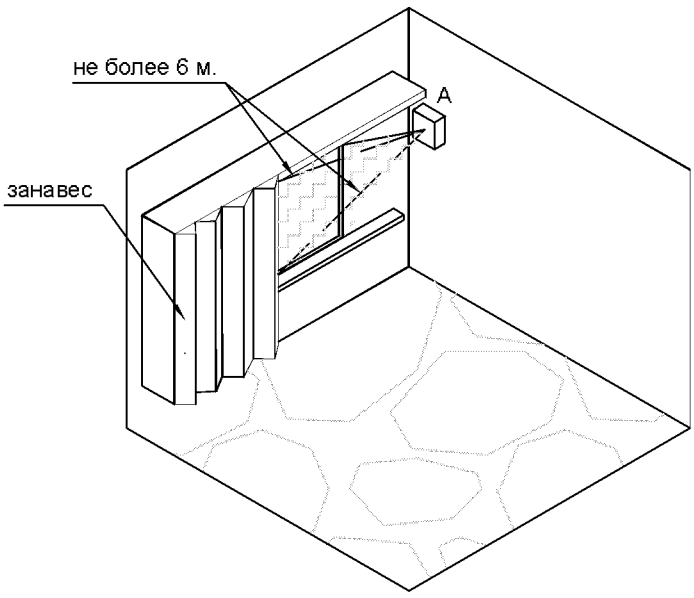
Приложение 4

Схема установки извещателя охранного поверхностного звукового (акустического)

Установка на потолке



Установка извещателя между стеклом и занавесом (жалюзи)

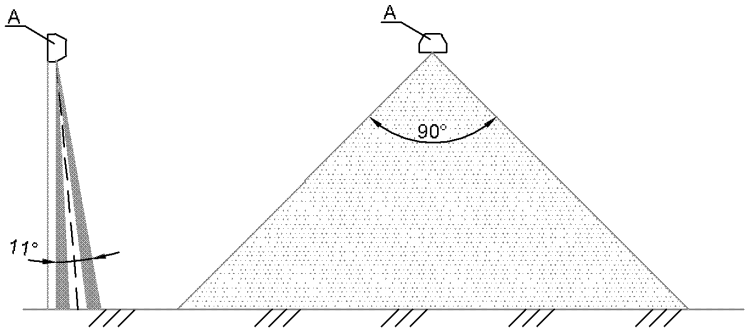


А-Извещатель охранный поверхностной звуковой (акустический)

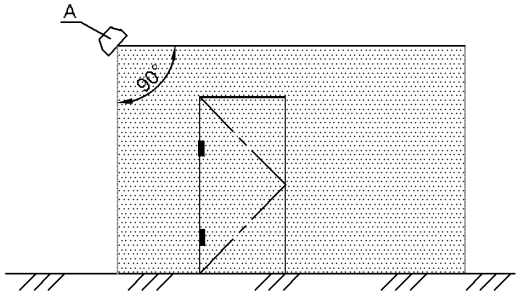
Приложение 5

Схема установки извещателя охранного поверхностного оптико-электронного (инфракрасного)

Зоны обнаружения



Зона обнаружения



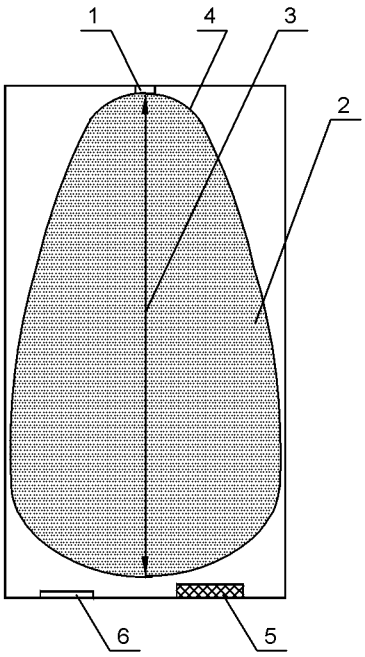
А-Извещатель охранный поверхностной оптико-электронный

Приложение 6

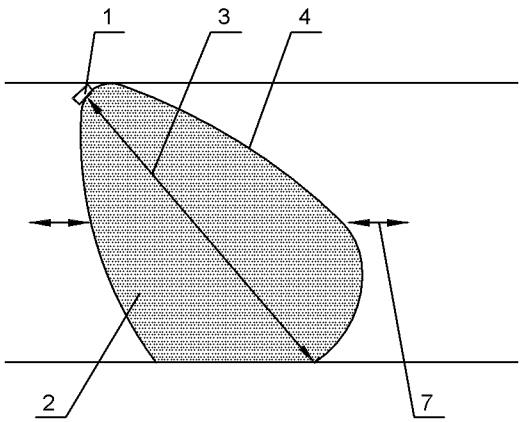
Схема установки извещателя охранного объемного ультразвукового

Вид сверху

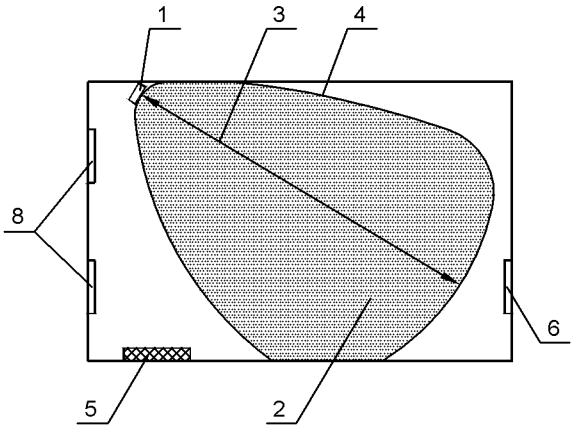
Вариант 1



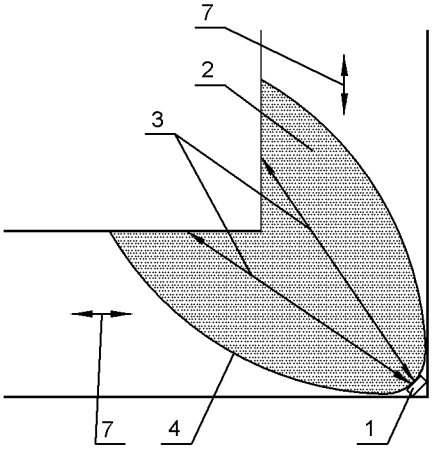
Вариант 2



Вариант 3



Вариант 4

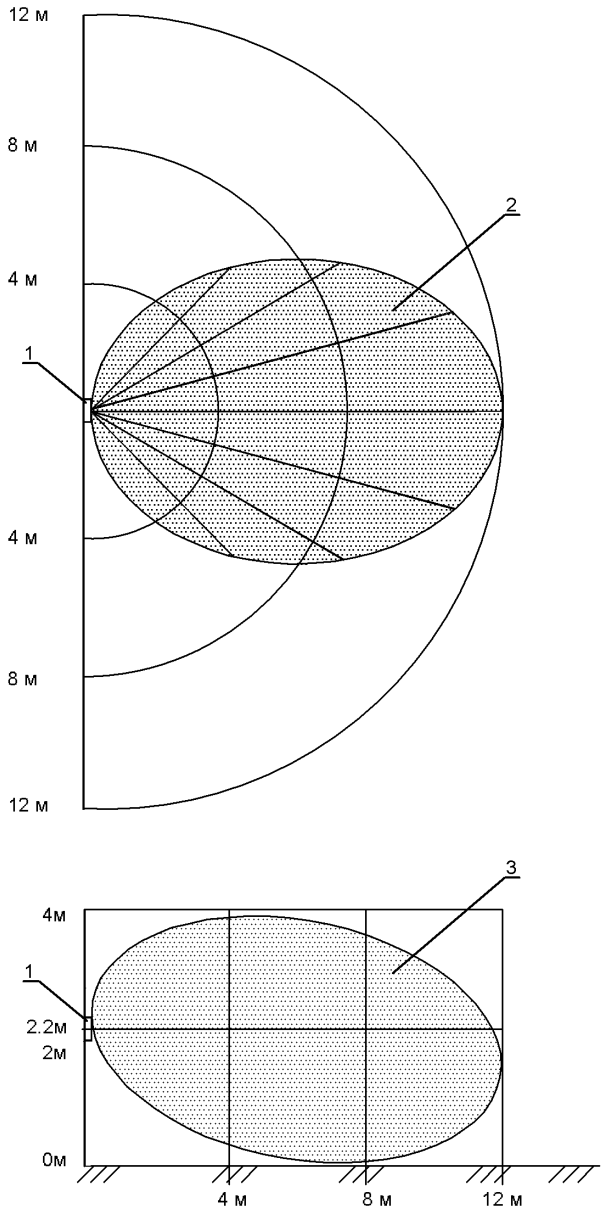


1-извещатель
2-зона обнаружения (ЗО)
3-дальность действия (осевая линия ЗО)
4-граница ЗО
5-электрообогреватель или батарея отопления
6-дверь
7-наиболее вероятное направление движения нарушителя
8-окно

Приложение 7

Схема установки извещателя охранного объемного радиоволнового

Зоны обнаружения



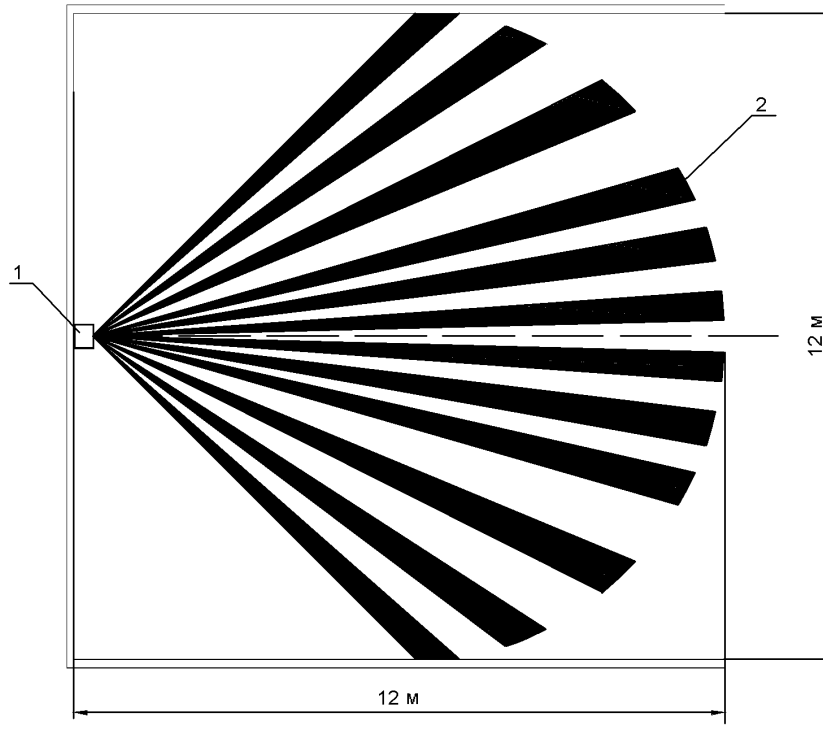
1-Извещатель охранный объемный радиоволновой
2-Зона обнаружения в горизонтальной плоскости
3-Зона обнаружения в вертикальной плоскости

Приложение 8

Схема установки извещателя охранного объемного оптико-электронного (инфракрасного)

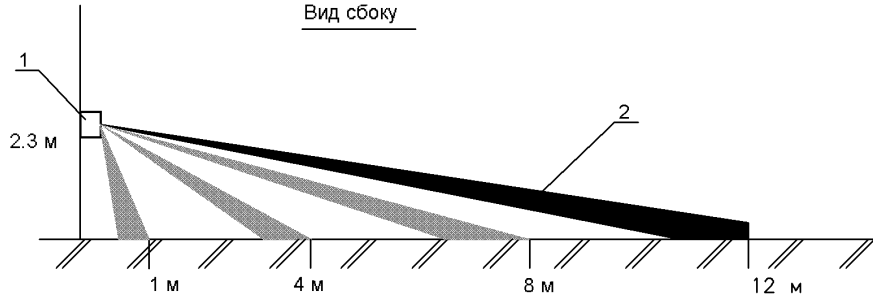
Зона обнаружения

Вид сверху



Зона обнаружения

Вид сбоку

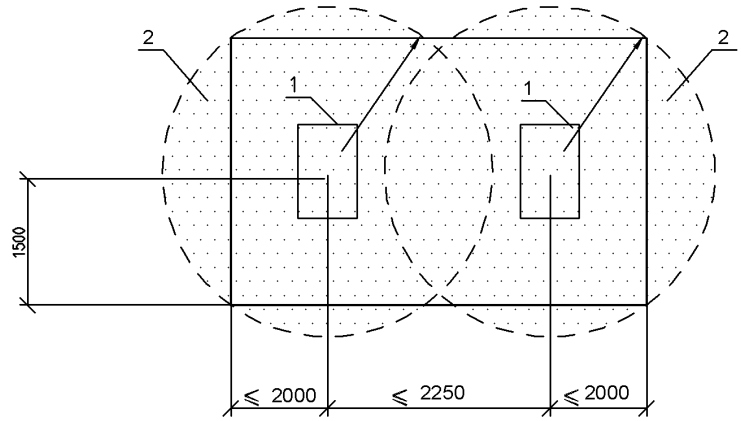


1-Извещатель охранный оптико-электронный (инфракрасный)
2-Зона обнаружения

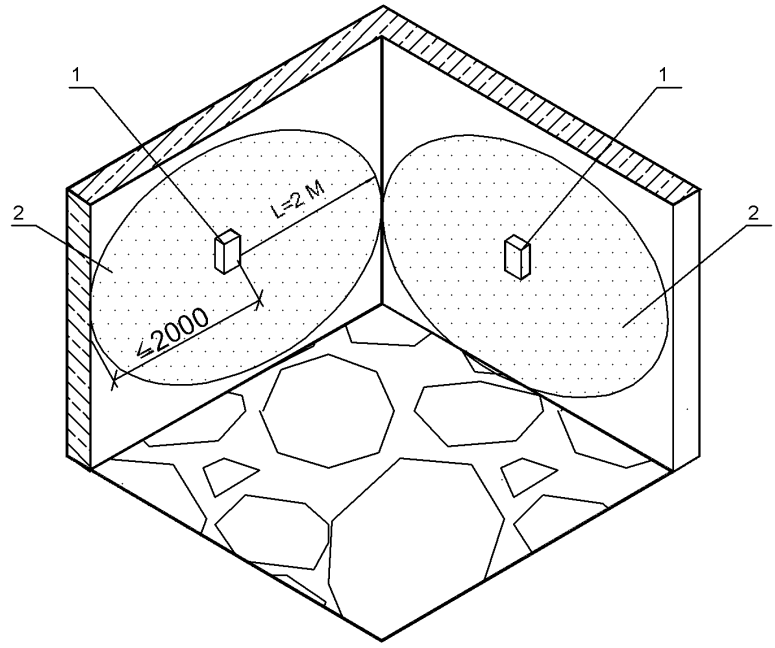
Приложение 9

Схема установки извещателя охранного поверхностного вибрационного на стене

Зоны обнаружения



Полная защита конструкции

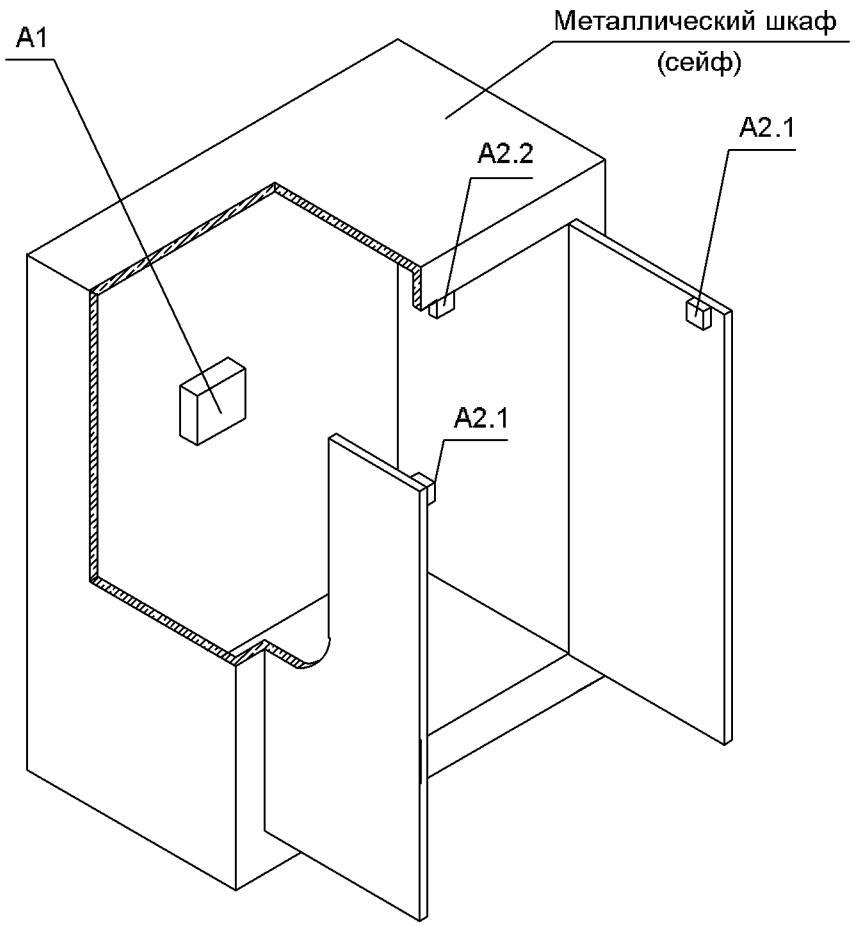


1- Извещатель охранный поверхностный вибрационный.

2- Зона обнаружения

Приложение 10

Схема установки извещателя охранного поверхностного вибрационного с датчиком наклона



A1- Извещатель охранный поверхностный вибрационный с датчиком наклона

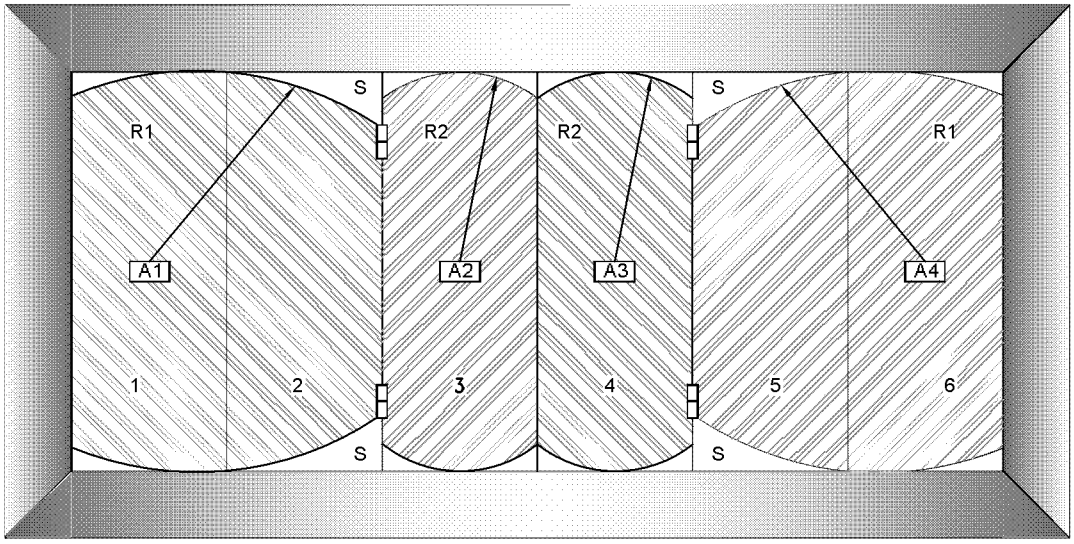
A2.1- Извещатель охранный магнитоконтактный (магнит)

A2.2- Извещатель охранный магнитоконтактный (геркон)

Все охранные извещатели устанавливаются внутри металлического шкафа

Приложение 11

Схема установки извещателя охранного поверхностного вибрационного многопозиционного для охраны немонолитной (многосекционной) конструкции



A1-A4 - многофункциональный вибрационный извещатель

R1- радиус действия для элементов конструкций 1,2 и 5,6, имеющих жесткую связь для передачи вибрации при разрушении

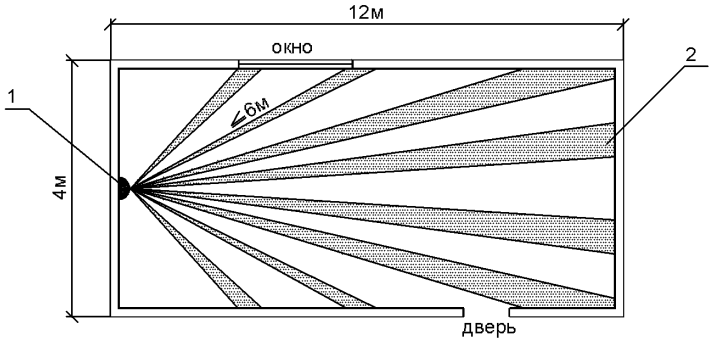
R2- радиус действия для элементов конструкций 3 и 4, не имеющих связи для передачи вибрации при разрушении

S - площадь, не охваченная радиусом R1 или R2($S < 0{,}1 м^2$)

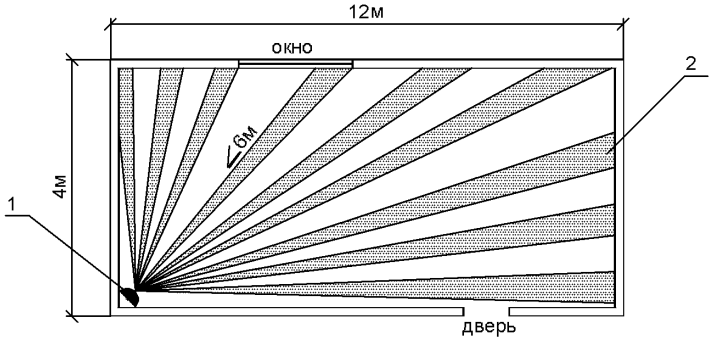
Приложение 12

Схема установки извещателя охранного объемного совмещенного (ИК+АК)

Установка на боковой стене



Установка в углу



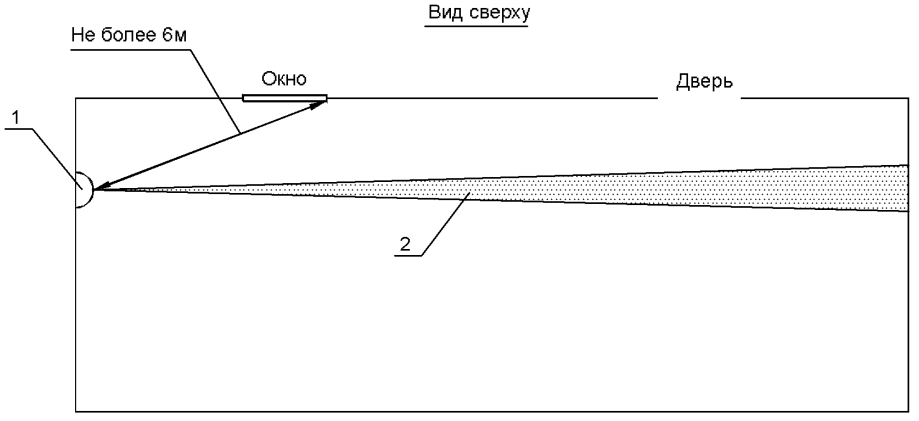
1- Извещатель охранный объемный совмещенный

2- Зона обнаружения

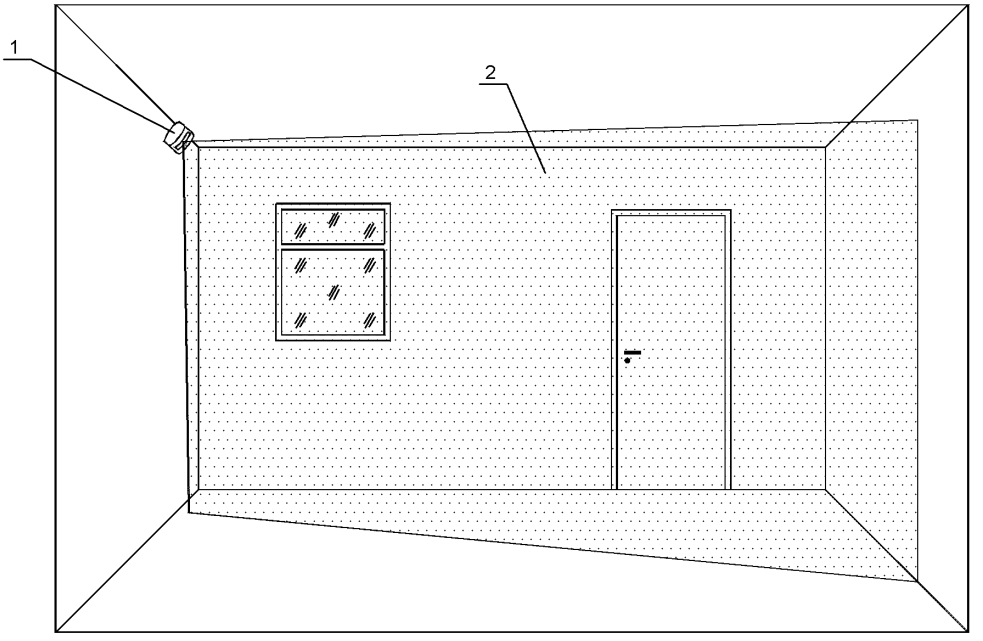
Приложение 13

Схема установки извещателя охранного поверхностного совмещенного (ИК+АК)

Вид сверху



Вид с боку

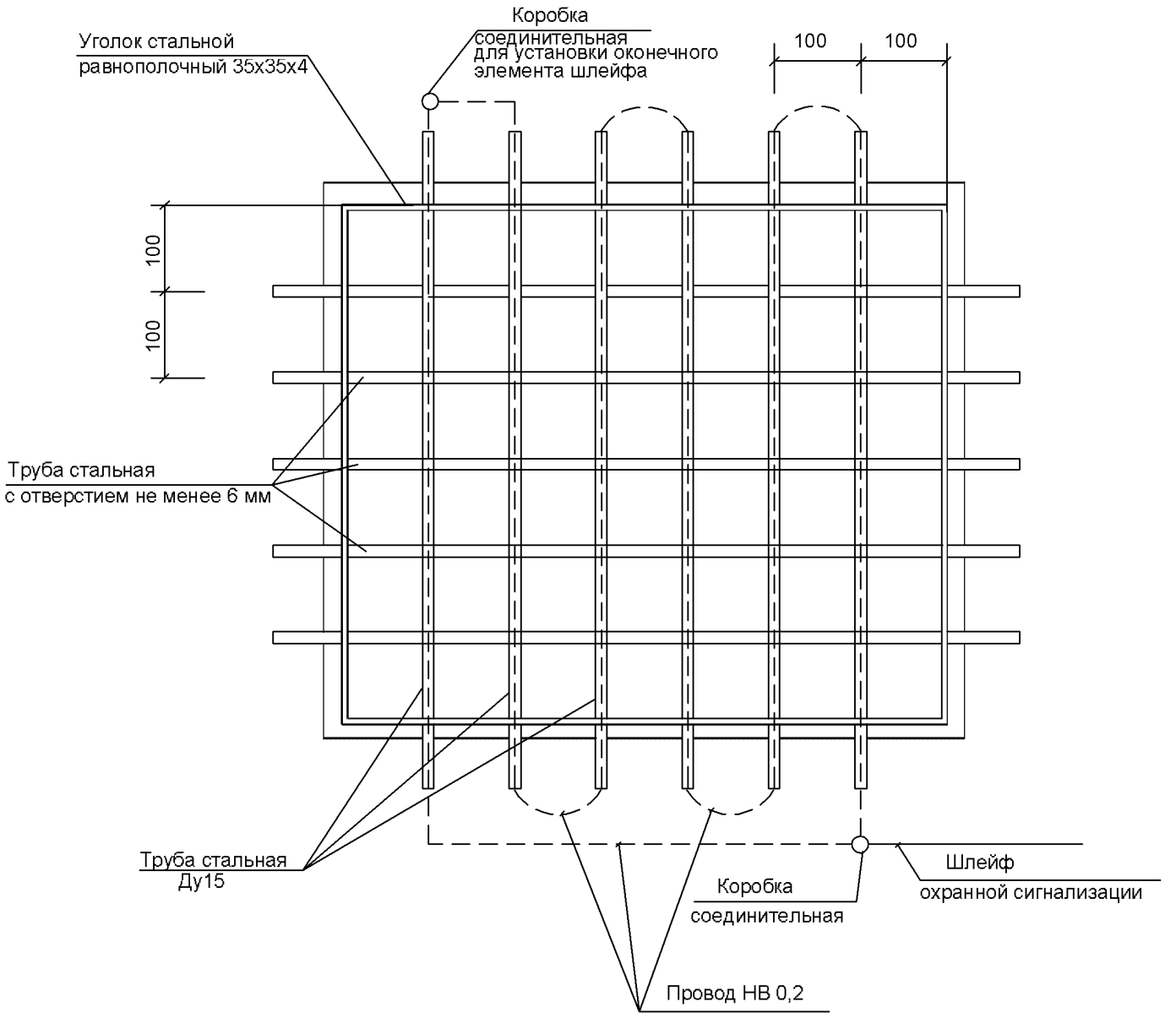


1- Извещатель охранный поверхностный совмещенный (ИК+АК).

2- Зона обнаружения ИК канала.

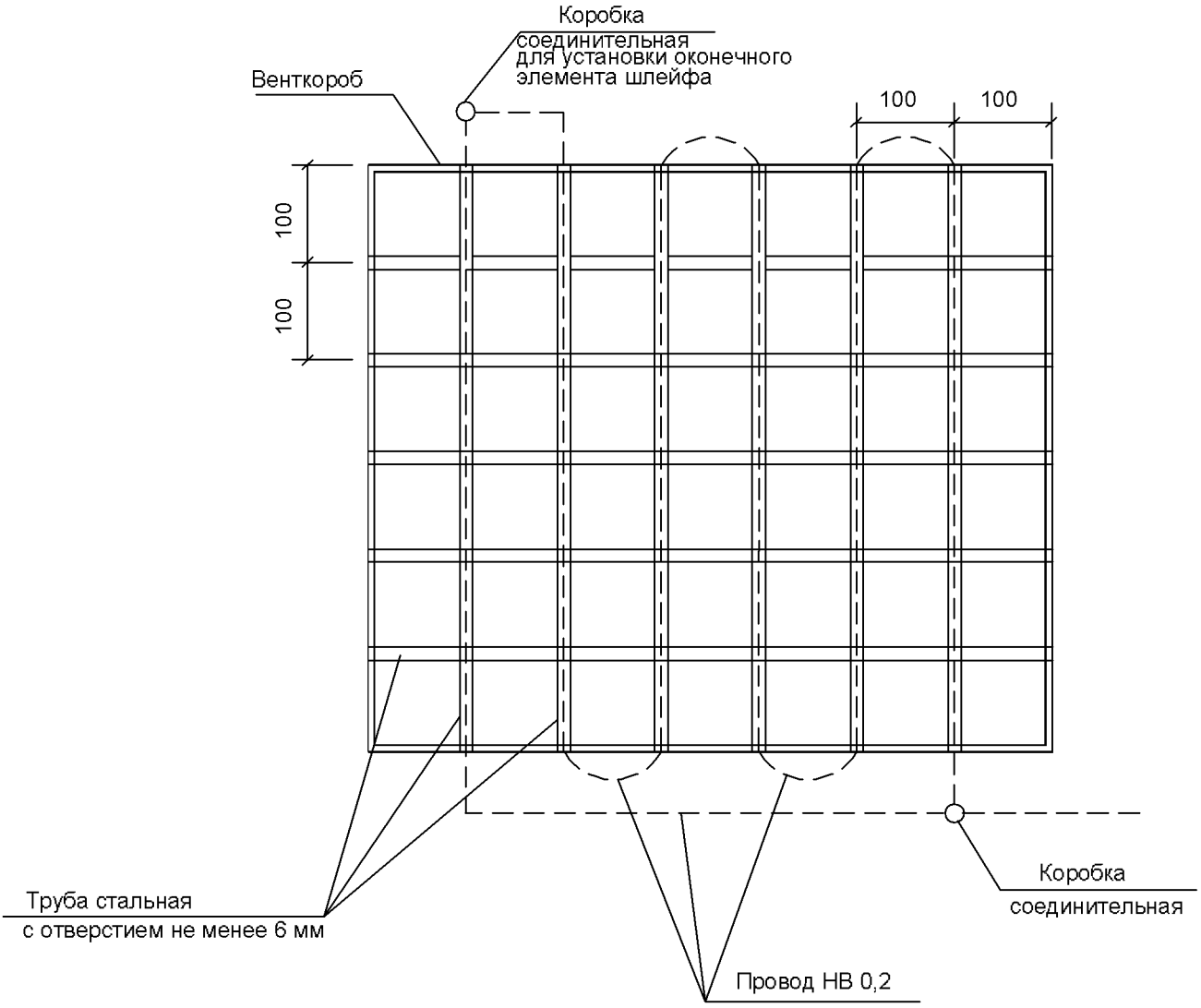
Приложение 14

Схема блокировки окна
омическим извещателем.



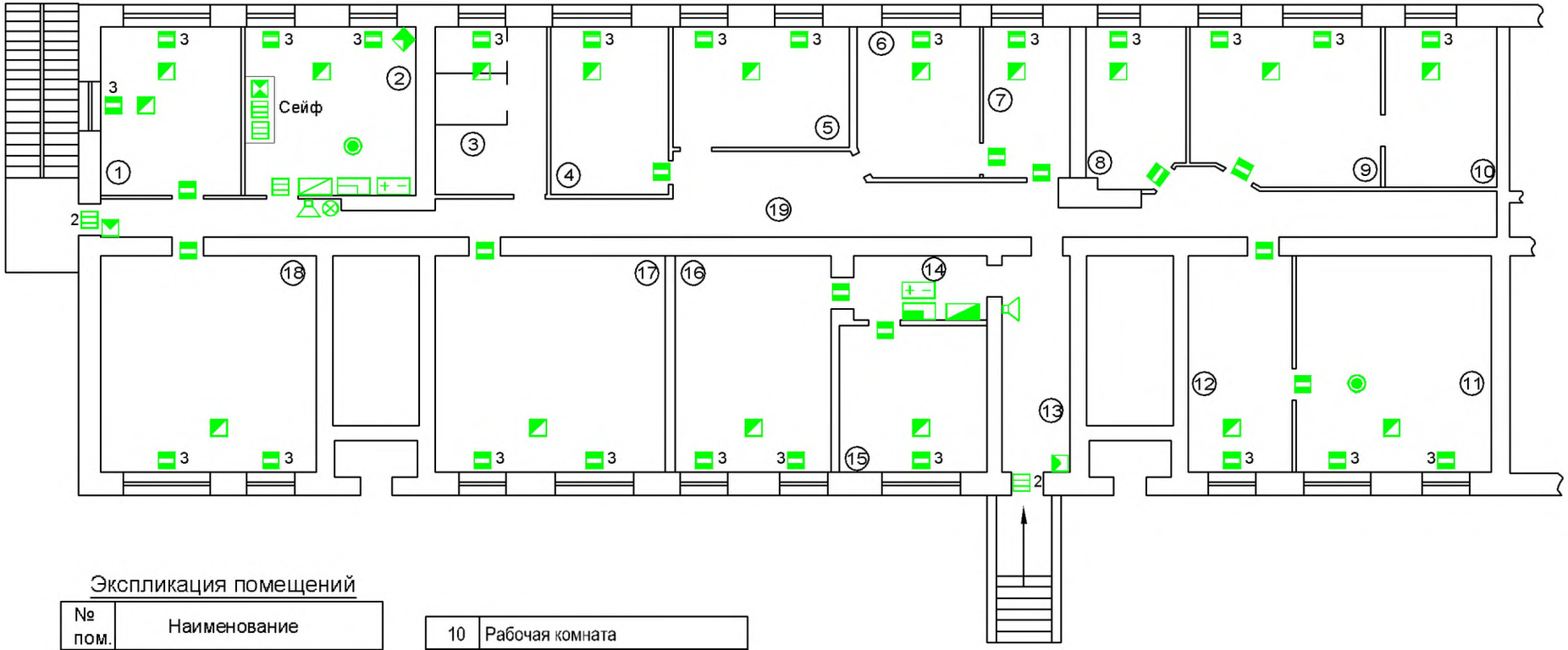
Приложение 15

Схема блокировки венткороба
омическим извещателем



План расположения оборудования СОТС в помещении ПЦО.

Приложение 16

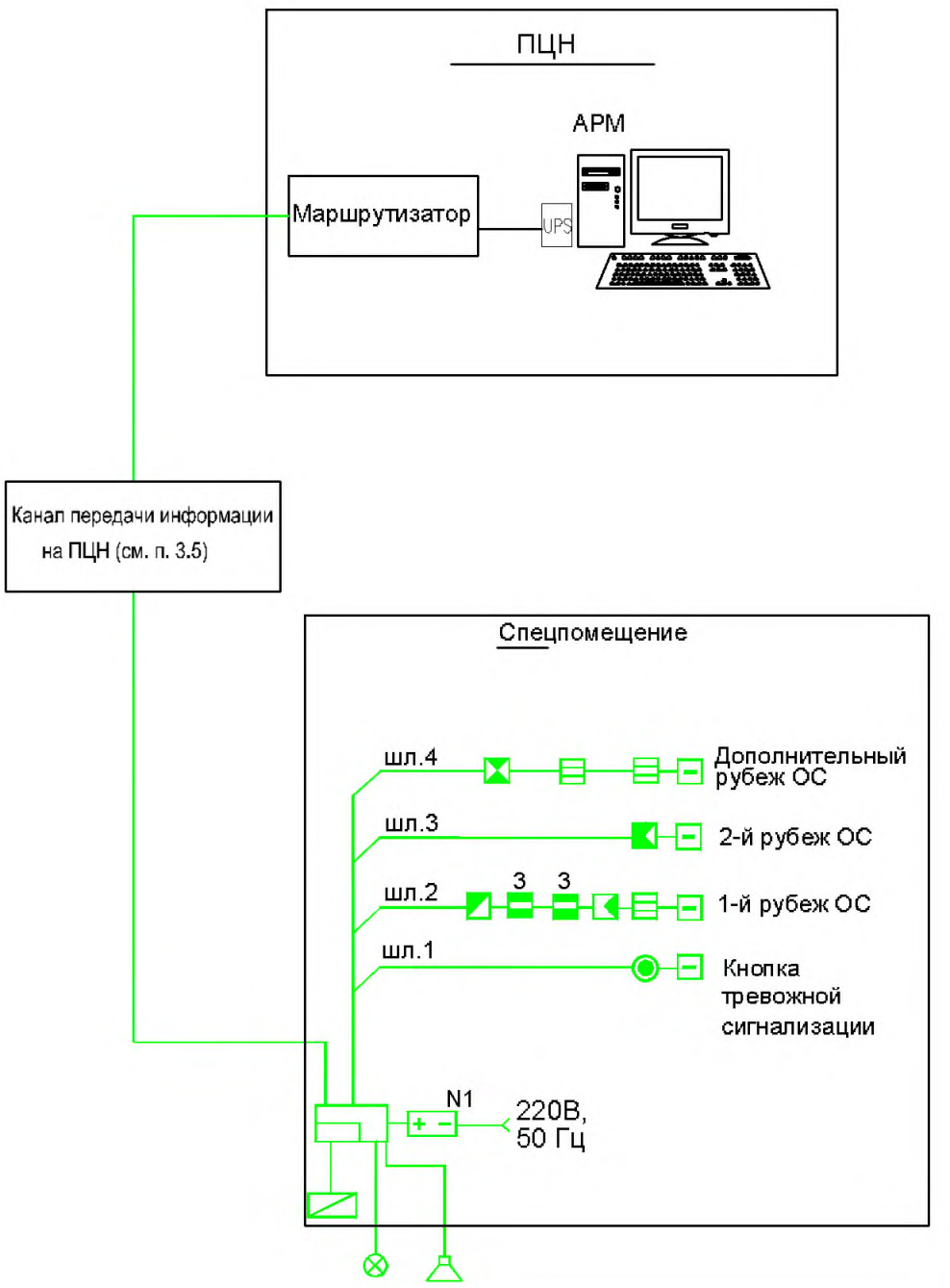


Экспликация помещений

№ пом.	Наименование
1	Рабочая комната
2	Спецпомещение
3	Туалет
4	Комната отдыха
5	ПЦО
6	ПЦО
7	Серверная
8	Рабочая комната
9	Рабочая комната

10	Рабочая комната
11	Кабинет начальника
12	Секретарь
13	Холл
14	Коридор
15	Квартирная группа
16	Бухгалтерия
17	Рабочая комноата
18	Кабинет заместителя начальника
19	Коридор

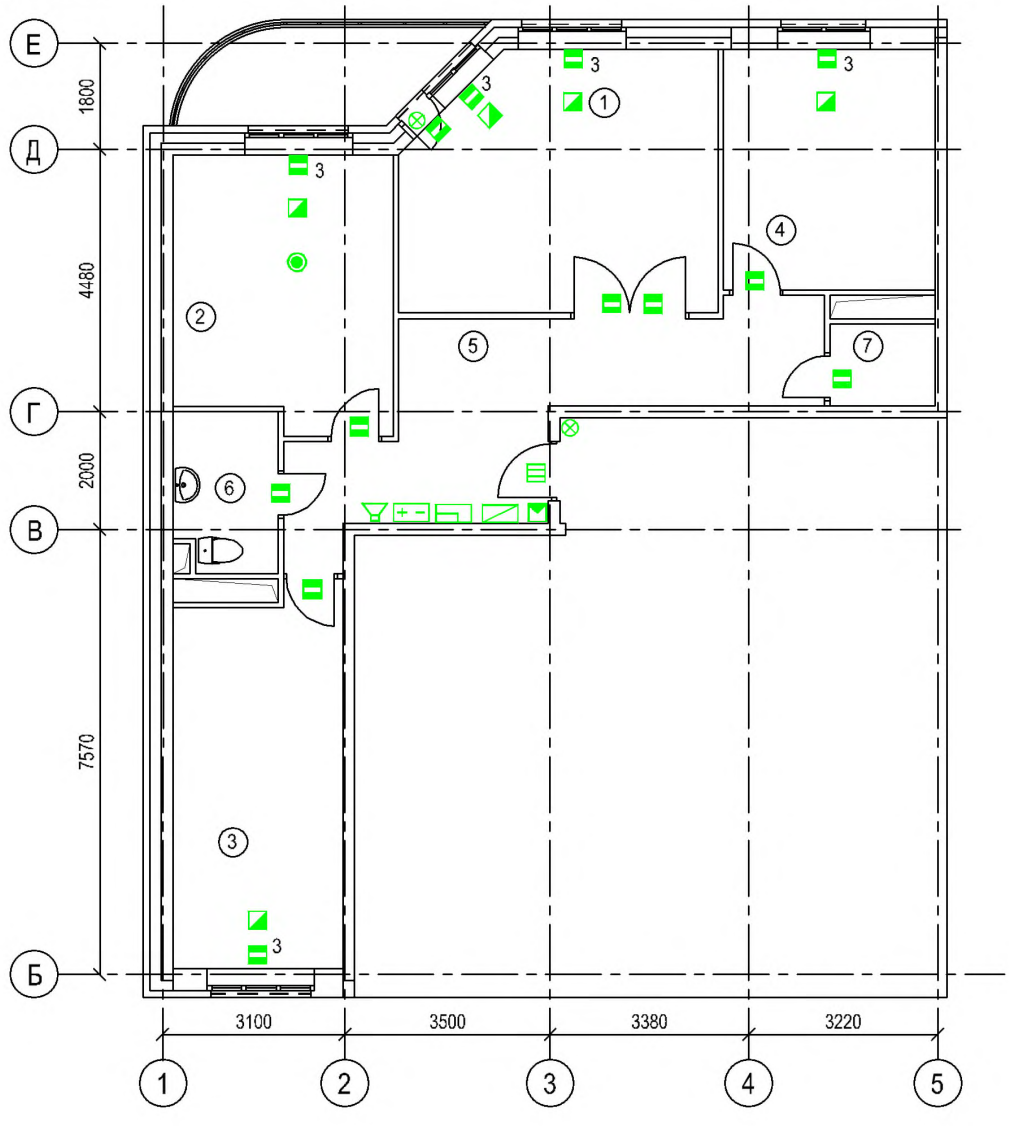
Схема структурная СОТС спецпомещения помещения.



Примечание

Оконечный элемент шлейфа сигнализации установить в конце шлейфа внутри корпуса охранного извещателя или в коробке соединительной КС

План расположения оборудования СОТС в помещении опорного пункта полиции.



Экспликация помещений

№ пом.	Наименование	Площадь м^2
1	Рабочая комната	22,8
2	Рабочая комната	17,1
3	Рабочая комната	18,3
4	Рабочая комната	14,8
5	Холл	20,3
6	Санузел	4,7
7	Кладовая	2,3

ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное казенное учреждение
«Научно-исследовательский центр «Охрана»

Методические рекомендации

«Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к четвертой категории»

Система контроля и управления доступом

РАЗДЕЛ 2

Москва 2016 г.

СОДЕРЖАНИЕ

1.	ОБЩАЯ ЧАСТЬ	55
2.	ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА	56
3.	СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ (СКУД)	57
3.1.	Типы и виды СКУД, их назначение и функции	57
3.2.	Функции СКУД в составе систем противокриминальной защиты объектов	59
3.3	Классификация СКУД	59
3.4	Составляющие СКУД	61
3.5	Электропитание СКУД	68
3.6	Выбор СКУД для оборудования объекта	69
3.7	Размещение и монтаж СКУД	70
3.8	Требования к минимально необходимому составу СКУД	72

ПРИЛОЖЕНИЯ

Приложение 1.	Условные обозначения.	75
Приложение 2.	План расположения оборудования СКУД в помещении ПЦО.	76
Приложение 3.	План расположения оборудования СКУД в помещении опорного пункта полиции.	77
Приложение 4.	Схема установки средств СКУД на одностворчатой двери.	78

1. ОБЩАЯ ЧАСТЬ.

Методические рекомендации по оснащению ведомственных объектов СКУД разработаны в соответствии со следующими нормативными правовыми актами и нормативно-техническими документами:

- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»;
- постановление Правительства Российской Федерации от 18 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»;
- постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищённости мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»;
- постановление Правительства Российской Федерации от 15 октября 1997 г. № 1314 «Об утверждении Правил оборота боевого ручного стрелкового и иного оружия, боеприпасов и патронов к нему, а также холодного оружия в государственных военизированных организациях» (с изменениями и дополнениями);
- приказ МВД России от 2.01.2013 № 1 «Об утверждении Концепции обеспечения собственной безопасности в системе Министерства внутренних дел Российской Федерации»
- приказ МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств»;
- приказ МВД России от 12 января 2009 г. № 13 «Об организации снабжения, хранения, учёта, выдачи (приёма) и обеспечения сохранности вооружения и боеприпасов в органах внутренних дел Российской Федерации»;
- приказ МВД России от 12 апреля 1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814» (вместе с «Инструкцией по организации работы органов внутренних дел по контролю за оборотом гражданского и служебного оружия и патронов к нему на территории Российской Федерации»);
- приказ МВД России от 12 апреля 2013 г. № 200дсп «О мерах по совершенствованию деятельности дежурных частей территориальных органов МВД России»;

- СП 12-95 «Инструкция по проектированию объектов органов внутренних дел (милиции) МВД России»;
- СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования»;
- ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»;
- ГОСТ Р 21.1101-2013 «СПДС. Общие требования к проектной и рабочей документации»;
- ГОСТ Р 54101-2010 «Средства автоматизации и системы управления. Средства и системы обеспечения безопасности. Техническое обслуживание и текущий ремонт»;
- Р 78.36.005-2011 «Выбор и применение систем контроля и управления доступом»;
- Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»;
- РД 78.145-93 «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приёмки работ»;
- Пособие к РД 78.145-93;
- Р 78.36.031-2013 «О порядке обследования объектов, квартир и МХИГ, принимаемых под охрану: Методические рекомендации»;
- Р 78.36.039-2014 «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения»;
- «Список технических средств безопасности, удовлетворяющих «Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны» (Действующая редакция);
- ПУЭ - Правила устройства электроустановок (издание 7).

2. ХАРАКТЕРИСТИКА ЗАЩИЩАЕМОГО ОБЪЕКТА.

В соответствии с пунктом 4.4 Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищённости объектов органов внутренних дел Российской Федерации от преступных посягательств, утверждённой приказом МВД России от 31.12.2014 г. № 1152, под объектом IV категории по степени потенциальной угрозы понимается обособленное помещение или группа

помещений, расположенных в зданиях или сооружениях, не относящихся к системе органов внутренних дел Российской Федерации, в которых ВР не требует осуществления ПР и круглосуточного дежурства

3. СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ.

Система контроля и управления доступом – совокупность программно-технических средств и организационно-методических мероприятий для санкционированного доступа в помещения (зоны) охраняемого объекта и регистрации фактов доступа и попыток несанкционированного доступа, а также оперативный контроль за санкционированным доступом на территории охраняемого объекта.

3.1 Типы и виды СКУД. Их назначение и функции.

СКУД классифицируются по:

- способу управления;
- количеству контролируемых точек доступа;
- функциональным характеристикам;
- уровню защищённости системы от несанкционированного доступа к информации.

По способу управления СКУД различают:

- автономные – для управления одним или несколькими устройствами преграждающими управляемыми (УПУ), без передачи информации на центральное устройство управления и без контроля со стороны оператора;
- централизованные (сетевые) – для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;
- универсальные (сетевые) – включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи.

По количеству контролируемых точек доступа:

- малой ёмкости (до 64 точек);
- средней ёмкости (от 64 до 256 точек);
- большой ёмкости (более 256 точек).

По функциональным характеристикам СКУД могут быть трёх классов:

1 - системы с ограниченными функциями;
2 - системы с расширенными функциями;
3 - многофункциональные системы.

Классификация средств и систем контроля и управления доступом по устойчивости к несанкционированным действиям (далее НСД).

Классификация средств СКУД по устойчивости к НСД определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости:

- нормальной;
- повышенной;
- высокой.

УПУ классифицируют по устойчивости к разрушающим воздействиям.

Устойчивость УПУ устанавливается по:

- устойчивости к взлому;
- пулестойкости (только для УПУ со сплошным перекрытием проема);
- устойчивости к взрыву.

Нормальная устойчивость УПУ обеспечивается механической прочностью конструкции без оценки по показателям устойчивости к разрушающим воздействиям.

Для УПУ повышенной и высокой устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и с блокированием объекта в проеме (шлюзы, кабины проходные) устанавливается классификация по устойчивости к взлому, взрыву и пулестойкости.

Устройства исполнительные (замки, защелки) классифицируют по устойчивости к разрушающим воздействиям в зависимости от конструкции.

По устойчивости к неразрушающим воздействиям средства КУД в зависимости от их функционального назначения классифицируют по следующим показателям:

- устойчивости к вскрытию – для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивости к манипулированию;
- устойчивости к наблюдению для считывателей ввода запоминаемого кода (клавиатуры, кодовые переключатели и т.п);
- устойчивость к копированию (для идентификаторов);
- устойчивости защиты средств вычислительной техники (СВТ) средств управления СКУД от несанкционированного доступа к информации.

Классификация систем КУД к НСД определяется для систем с централизованным управлением по защищенности от несанкционированного доступа к информации программного обеспечения СКУД и СВТ, входящих в состав сетевых СКУД.

3.2 Функции СКУД в составе систем противокриминальной защиты объектов.

СКУД применяются для предотвращения несанкционированного доступа людей, транспорта и других объектов в зону (из зоны) доступа (здания, помещения) в целях обеспечения противокриминальной защиты объектов.

СКУД действуют по принципу сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту, с информацией, заложенной в памяти системы.

СКУД должна выполнять следующие функции:

санкционирование – процедура присвоения каждому пользователю персонального идентификатора, кода, регистрацию его в системе (или регистрацию его биометрических признаков) и задание для него временных интервалов и уровня доступа (в какие помещения, когда и кто имеет право заходить);

идентификацию – процедуру опознавания пользователя по предъявленному идентификатору или биометрическому признаку;

авторизацию – проверку полномочий, заключающуюся в проверке соответствия времени и уровня доступа установленным в процессе санкционирования;

аутентификацию – установление подлинности пользователя по признакам идентификации;

разрешение доступа или отказ в доступе – выполняется на основании результатов анализа предыдущих процедур;

регистрация – протоколирование всех действий в системе;

реагирование – реакция системы на несанкционированные действия (подача предупреждающих и тревожных сигналов, отказ в доступе и т.д.).

3.3 Классификация СКУД.

1-й класс - системы с ограниченными функциями.

К СКУД 1-го класса относятся малофункциональные системы малой ёмкости, работающие в автономном режиме. Такие системы применяются в случае, если на объекте необходимо обеспечить контролируемый доступ сотрудников и посетителей, имеющих соответствующий идентификатор. При этом не ставится задача контроля времени доступа и выхода из помещения, регистрация проходов, передача данных на центральный компьютер.

Автономная система состоит из контроллера, обычно объединённого со считывателем, и исполнительного элемента. Как правило, используются магнитные (реже бесконтактные) карточки, электронные ключи "TouchMemory". В зависимости от типа контроллера количество лиц в списках может достигать от 60 до 2800 человек. Автономные системы снабжаются резервным питанием и имеют механический ключ для открывания замка в аварийных ситуациях.

Устанавливаются на объектах, где требуется только ограничение доступа посторонних лиц (функция замка).

2-й класс - системы с расширенными функциями.

СКУД 2-го класса – монофункциональные системы (одноуровневые и многоуровневые системы, работающие в автономном или сетевых режимах).

СКУД малой и средней ёмкости, но с возможностью расширения и включения их или их составных частей в общую линию связи (сетевой режим).

Данные системы имеют ряд дополнительных функций:

– ограничение допуска в охраняемую зону конкретного лица, группы лиц по дате и временным интервалам в соответствии с имеющимся идентификатором;

– автоматическую регистрацию событий в собственном буфере памяти, выдачу тревожных извещений (при несанкционированном проникновении, неправильном наборе кода или взломе заграждающего устройства или его элементов) на внешние оповещатели или внутренний пост охраны;

– автоматическое управление открытием/закрытием устройства заграждения.

Они устанавливаются на объектах, где требуется учёт и контроль присутствия сотрудников в разрешённой зоне, в качестве дополнения к имеющимся на объекте системам охраны и защиты.

На объектах, оборудованных средствами и системами охранно-пожарной сигнализации (ОПС), СКУД 2-го класса применяются как самостоятельные системы, и они часто рассматриваются только как средства усиления режима обеспечения безопасности объекта.

3-й класс – многофункциональные системы.

СКУД 3-го класса (сетевые). Контроллеры систем данного класса объединены в локальную сеть, работающую в реальном времени и ведущую непрерывный диалог с периферийными устройствами, с ведущим контроллером или с управляющим компьютером, расположенным в пункте охраны. Системы этих классов – крупные многоуровневые системы, рассчитанные на большое число пользователей (1500 человек и более).

Подобные системы применяются в случае, когда необходимо контролировать время прохода сотрудников и посетителей на объект и в помещения. При этом применяются более сложные электронные идентификаторы (Proximity, Виганд карточки, биометрический контроль или их сочетание). Время прохода на каждый день недели и для каждого владельца электронной карточки задаётся администратором системы.

Системы 3-го класса обычно интегрируются с системами охранно-пожарной сигнализации и системами телевизионного наблюдения на релейном уровне. Релейный уровень предполагает наличие дополнительного модуля в контроллере (или дополнительных входов/выходов в контроллере), к которому подключаются охранные или пожарные извещатели и релейные выходы для управления телекамерами и другими устройствами. Подобная интеграция применяется, в основном, на малых объектах. На таких объектах количество взаимодействий между системами невелико, и все они могут быть учтены в процессе проектирования системы безопасности. Этот уровень интеграции является простым, универсальным и достаточно надёжным.

3.4 Составляющие СКУД.

Устройства преграждающие управляемые – устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (двери, оборудованные исполнительными устройствами СКУД).

Устройства исполнительные (УИ) – устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние устройств преграждающих управляемых (электромеханические, электромагнитные замки, электромагнитные защёлки, механизмы привода шлюзов, ворот, турникетов и другие подобные устройства).

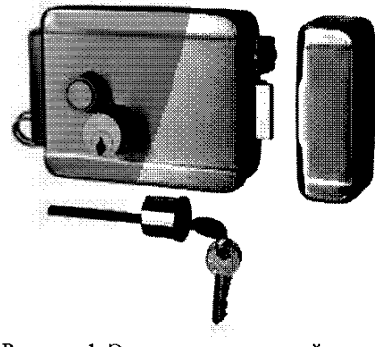


Рисунок 1. Электромеханический замок.

Электромеханический принцип действия исполнительного механизма замка основан на перемещении закрывающих элементов (запоров, ригелей замков и т.п.) с помощью включения на время их передвижения электромотора или электромагнита (Рисунок 1).

В исполнительных механизмах с электромагнитным принципом действия отсутствуют движущиеся механические закрывающие элементы, то есть блокировка устройств заграждения (например, дверей) осуществляется с помощью сил магнитного притяжения, создаваемых мощным магнитом.

Часто в электромеханических замках применяют электромагнитную блокировку (магнитные защёлки, задвижки и т.п.) закрывающих элементов с возможностью перемещения их вручную при открывании или закрывании в экстремальных условиях.

Электромеханический замок рекомендуется устанавливать на деревянных и/или металлических дверях массой до 100 кг при условии средней нагруженности (100 – 200 проходов в день). Применение этого замка для дверей с высокой нагруженностью неэффективно из-за высокого механического износа и, как следствие, снижения надёжности и срока службы. Чаще всего электромеханический замок устанавливают на двери (накладной или врезной замок), но иногда его устанавливают и на дверной коробке.

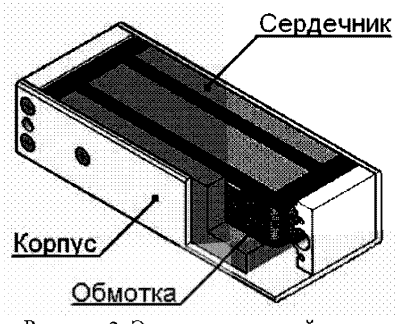


Рисунок 2. Электромагнитный замок.

Электромагнитный замок (Рисунок 2) рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг при условии высокой нагруженности (более 200 проходов в день). Отсутствие деталей, подверженных трению и износу, делает этот замок практически вечным.

Особенностью данного замка является необходимость постоянной подачи тока на обмотку электромагнита, при пропадании напряжения в сети (например, при аварии или умышленном обрыве проводов) замок открывается. В связи с этим для надёжной работы необходимо дублировать электромагнитный замок механическим или применять дополнительное резервное питание.

Электромагнитную защёлку рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери (при её закрывании), и разблокировать замок при подаче сигнала управления на открывание двери. Такая установка защёлки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромагнитные замки с плоским якорем выпускают двух видов: с якорем, работающим на отрыв, и с якорем, работающим на сдвиг. В обесточенном состоянии все замки нормально открыты. Замки с якорем "на отрыв" изготавливают в накладном варианте, а с якорем "на сдвиг" – в накладном и врезном вариантах.

Для входных дверей используют электромагнитные замки с силой удержания от 200 до 600 кг, при этом ток потребления таких замков (при напряжении питания 12 В) составляет от 200 до 500 мА.

Помимо прямоугольных электромагнитных замков освоен выпуск круглых замков. Это позволило упростить изготовление и снизить стоимость. К недостаткам электромагнитных замков следует отнести потерю работоспособности при образовании зазора между электромагнитом и пластиной. Во избежание такой ситуации пластину укрепляют на резиновой прокладке, компенсирующей образующийся зазор.

Требование обеспечения соприкосновения электромагнита и пластины без зазора для обеспечения работоспособности замка, вызывает

необходимость обязательного применения качественного дверного доводчика.

Функция доводчика – не только гарантировать закрытие двери, но также оберегать замок от механических ударов.

Электромагнитные замки с плоским якорем имеют очень высокую надёжность, это определяется, в основном, конструкцией замка и в значительной степени – отсутствием трущихся деталей, износ которых ограничивает долговечность. Ударные нагрузки, возникающие при закрывании двери (особенно, если дверной доводчик плохо отрегулирован), и перепады температуры создают тяжёлые условия для элементов электроники. Поэтому их размещают вне корпуса замка.

Устройства считывающие (УС).

УС – это устройство, предназначенное для считывания (ввода) идентификационных признаков с целью опознания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. По принципу считывания они могут быть:

- с ручным вводом;
- контактные;
- бесконтактные;
- биометрические;
- комбинированные.

Идентификаторы (ИД) (носитель идентификационного признака).

Идентификатор – это уникальный признак субъекта или объекта. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код – предмет, в котором (на который) с помощью специальной технологии занесён идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и другие устройства).

Разновидности идентификаторов.

Механические – представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей).

К механическим идентификаторам относятся такие устройства, как кодовые панели и механические ключи. Механические идентификаторы просты и имеют несколько недостатков: простота подделки, наличие движущихся частей, которые снижают надёжность, невозможность использования для идентификации личности.

Магнитные – представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда) (Рисунок 3).

Данная технология получила широкое распространение в системах контроля и управления доступом благодаря относительной сложности подделки идентификаторов, возможности применения карт в качестве

идентификаторов личности. Магнитные системы позволяют разграничивать доступ для большого числа пользователей (до 2000 и более).

Оптические – представляют собой нанесённые на поверхность или внутри идентификатора метки, имеющие различные оптические характеристики (карты со штрих кодом, голографические метки) (Рисунок 4).

Электронные контактные – представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи) (Рисунок 5).



Рисунок 3. Карта доступа с магнитной полосой.



Рисунок 4. Карта доступа со штрих кодом.



Рисунок 5. Электронная карта доступа.

Электронный ключ TouchMemory представляет собой металлическую "таблетку" небольшого диаметра толщиной 4-6 мм, внутри которой запрессована электронная микросхема с уникальным 48-разрядным кодом. "Таблетка" не имеет собственного источника питания, а заряжается от считывателя при соприкосновении с ним. И ключ, и считыватель

изготавливаются в герметичном исполнении, что делает их практически вечными. Они надёжны в работе, имеют высокую устойчивость к электромагнитным и криминальным воздействиям. Для удобства пользования "таблетка" закрепляется в пластмассовой пластинке, имеющей отверстие для подвешивания её на одну связку с другими ключами (Рисунок 6).



Рисунок 6. Электронные ключи TouchMemory.

Карточка бесконтактная (Proximity) – карточка, с которой информация о коде ключа считывается радиочастотным способом на расстоянии (то есть без непосредственного контакта со считывателем). Различают пассивные и активные карточки. Пассивные карточки питаются энергией, получаемой от считывателя, и действуют на расстоянии до 10 см (Рисунок 7).



Рисунок 7. Карточка бесконтактная (Proximity).

Активные – имеют встроенную батарейку, срок работы которой составляет до 10 лет. Считыватель размещается, как правило, скрытно в полости неметаллической двери или за радиопрозрачной стенкой. В пассивных карточках информация записывается один раз на всё время действия карточки, а в активных существует возможность ее изменения.

Электронные радиочастотные – считывание кода с электронных идентификаторов происходит путём передачи данных по радиоканалу.

Акустические – представляют собой кодированный акустический сигнал.

Средства управления (аппаратные устройства).

Контроллер доступа (КД) и прибор приемно-контрольный доступа (ППКД) представляют собой аппаратное устройство в составе средств управления системы контроля и управления доступом (Рисунок 8).

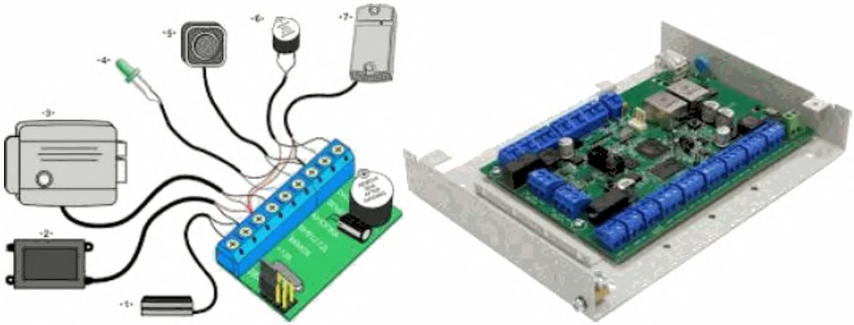


Рисунок 8. Контроллер доступа.

Автономный – для управления одним или несколькими устройствами преграждающими управляемыми без передачи информации на центральное устройство управления и контроля со стороны оператора.

Централизованный (сетевой) – для управления устройствами преграждающими управляемыми с обменом информацией с центральным пультом и контролем управления системой со стороны центрального устройства управления.

Универсальный (сетевой) – включает в себя функции как автономных, так и сетевых систем, работающих в сетевом режиме под управлением центрального устройства управления, переходящий в автономный режим при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи.

Домофоны.

Домофон – устройство для управления доступом с возможностью дистанционного управления сотрудником дежурной смены на основе получаемой аудио/видеоинформации (Рисунок 9).

Домофоны сочетают в себе функции аудио- и/или видеоконтроля и управления доступом на объекте. Домофоны позволяют абоненту, не подходя к двери, идентифицировать посетителя по изображению и/или голосу и дистанционно управлять входной дверью.

Домофон позволяет, соблюдая безопасную дистанцию между посетителем и охраной объекта, выяснить требующуюся информацию о посетителе и принять взвешенное решение о его допуске на объект.

При выборе домофона необходимо обращать особое внимание на его климатическое исполнение, антивандальные свойства, надёжность.



Рисунок 9. Домофоны.

По виду (способу идентификации посетителей) домофоны подразделяются на:

аудиодомофоны – обеспечивают двухстороннюю аудиосвязь абонента с посетителем и позволяют идентифицировать посетителя по его голосу.

Видеодомофоны – обеспечивают видеоконтроль наружного околодверного пространства, двухстороннюю аудиосвязь абонента с посетителем и позволяют идентифицировать посетителя по его изображению и голосу.

По количеству обслуживаемых абонентов различают:

Индивидуальные (одноабонентские) – домофоны позволяют обслуживать только одного абонента и применяют для защиты отдельных квартир, небольших офисов, загородных домов, а также могут быть установлены на постах охраны.

Видеодомофон обеспечивает более высокий уровень безопасности абонента, чем аудиодомофон, так как (помимо двухсторонней аудиосвязи) позволяет получить телевизионное изображение посетителя.

При выборе домофона следует обращать особое внимание на такие факторы:

– климатическая устойчивость, прежде всего – диапазон рабочих температур, который должен быть для некоторых блоков (например, блока вызова, электрозамка, доводчика двери) не менее минус 40÷плюс 40° С;

– устойчивость к вандализму;

– устойчивость к нестабильному электропитанию;

– наличие сертификата соответствия;

– обязательное наличие полной эксплуатационной документации с принципиальными и монтажными схемами на русском языке;

– наличие стабильного гарантийного и послегарантийного обслуживания предлагаемого оборудования и возможность закупки ремонтных ЗИП.

3.5 Электропитание СКУД.

Основное электропитание СКУД должно осуществляться от сети переменного тока частотой 50 Гц номинальным напряжением 220 В.

СКУД должна быть работоспособна при допустимых отклонениях напряжения сети от минус 15% до плюс 10%.

Электропитание отдельных средств СКУД допускается осуществлять от других источников с иными параметрами выходных напряжений, требования к которым устанавливают в нормативных документах на СКУД конкретных типов.

СКУД должны быть обеспечены резервным электропитанием при пропадании напряжения основного источника электропитания.

В качестве резервного источника электропитания может использоваться резервная сеть переменного тока или источники постоянного тока.

Переход на резервное электропитание должен осуществляться автоматически без нарушения установленных режимов работы и функционального состояния средств СКУД.

Резервный источник электропитания должен обеспечивать выполнение основных функций системы при пропадании напряжения в сети:

Системы 1 класса – 0,5 ч.

Системы 2 класса – 0,5 ч.

Система 3 класса – 1 ч.

Допускается не применять резервирование электропитания с помощью аккумуляторных батарей для УПУ, которые требуют для управления значительных мощностей приводных механизмов (приводы ворот, шлюзы).

При этом такие УПУ должны быть оборудованы аварийными механическими средствами открывания и системными средствами индикации аварии электропитания.

При использовании в качестве источника резервного электропитания СКУД аккумуляторных или сухих батарей рекомендуется иметь индикацию разряда батареи ниже допустимого предела.

Химические источники электропитания, встроенные индикаторы или обеспечивающие сохранность данных в контроллерах, должны обеспечивать работоспособность СКУД в течение не менее трёх лет.

3.6 Выбор СКУД для оборудования объекта.

Выбор варианта оборудования объекта средствами СКУД следует начинать с его обследования.

Основными целями первичного обследования являются:

- определение размера возможного ущерба предприятию (организации) или собственнику имущества и связанной с ним категории объекта.

По результатам обследования определяются тактические характеристики и структура СКУД, а также составляется техническое задание на оборудование объекта СКУД. В техническом задании указывается:

- назначение СКУД, техническое обоснование и описание системы;
- размещение составных частей системы;
- условия эксплуатации средств СКУД;
- основные технические характеристики, такие, как:
  - пропускная способность в охраняемые зоны, особенно в час-пик;
  - максимально возможное число пользователей на один считыватель;
  - максимальное число и виды идентификаторов;
  - требования к маскировке и защите средств СКУД от вандализма;
- оповещение о тревожных и аварийных ситуациях и принятие соответствующих мер по их пресечению или предупреждению;
- возможность работы и сохранения данных без компьютера или при его отказе;
- алгоритм работы системы СКУД в аварийных и чрезвычайных ситуациях;
- программное обеспечение системы;
- требования к безопасности;
- требования к электропитанию;
- обслуживание и ремонт системы;
- требования к возможности включения системы СКУД в интегрированную систему безопасности.

Путём изучения чертежей, обхода и осмотра объекта, а также проведения необходимых измерений определяются:

- количество входов/выходов и их геометрические размеры (площадь, линейные размеры, пропускная способность и т.п.);
- материал строительных конструкций;
- количество отдельно стоящих зданий, их этажность;
- количество открытых площадок;
- количество отапливаемых и неотапливаемых помещений и их расположение.

Учитывать вредное воздействие окружающей среды следует лишь для исполнительных устройств, считывателей и контроллеров (совмещенных со считывателями в одном конструктивном блоке), предназначенных для работы вне отапливаемых закрытых помещений либо в особых условиях (запылённость, повышенная влажность, отрицательная температура, агрессивная среда и т. п.). Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, удалённость считывателей и контроллеров от управляющего центра, заземление составных частей системы и т.п.

3.7 Размещение и монтаж СКУД.

Устройства центрального управления.

Устройства центрального управления (персональные компьютеры), являющиеся "мозгом" СКУД, рекомендуется устанавливать в отдельных служебных помещениях, защищённых от доступа посторонних лиц, например, в помещении дежурной части.

Основные положения, в соответствии с которыми разрабатываются режимы работы всей системы безопасности, определяются руководящим составом объекта, исходя из общей концепции обеспечения безопасности объекта. Управляющие программы загружаются в центральный управляющий и вспомогательные компьютеры или контроллеры и защищаются секретными кодами.

Персонал охраны, а также других служб, которые подключены к общей компьютерной сети, не должны иметь доступа к программным средствам и возможности влиять на установленные режимы работы, за исключением лиц, ответственных за данные работы.

При объединении компьютеров в сеть целесообразно разделять функциональные возможности среди пользователей сети и в соответствии с этим размещать компьютеры в помещениях объекта.

Устройства контроля и управления.

Ведущие контроллеры и контроллеры, работающие на несколько устройств заграждения, рекомендуется размещать в специальных запираемых металлических шкафах или нишах, на высоте, удобной для технического обслуживания. При этом следует дверцы данных шкафов или ниш блокировать охранной сигнализацией на возможное открытие или пролом.

Корпус данных контроллеров должен быть выполнен из ударопрочного материала, защищающего контроллер от актов вандализма. Контроллеры, управляющие работой считывателей или исполнительных устройств одной двери в двух направлениях, рекомендуется устанавливать с внутренней стороны охраняемого помещения.

При работе устройств контроля и управления в сетевом режиме необходимо учитывать возможность появления помех и сбоев в работе из-за неправильного монтажа соединительных линий и их длины.

Для нормальной работы рекомендуется:

– при значительной длине соединительного кабеля подключать к шине оконечные и согласующие элементы. Необходимое точное значение величины этих элементов зависит от характеристик кабеля;

– заземлять устройства и экранированные оплётки кабелей в одной точке (во избежание возникновения блуждающих токов), желательно у ведущего контроллера. При большой длине кабелей заземление можно производить в разных точках, но при этом обязательно использовать специальные методы и устройства защиты от помех;

– использовать шинные усилители при большой длине кабеля.

Считыватели и устройства исполнительные.

В зависимости от типа считывателей и устройств исполнительных, пропускной способности и организации системы безопасности объекта в целом, они могут устанавливаться как вблизи устройств заграждения, так и непосредственно на них. При их размещении необходимо учитывать условия эксплуатации, удобство монтажа, надёжность и вандалостойкость.

Считыватели "Proximity" удобнее всего размещать на стене, скрытно в стене перед устройствами заграждения или с внутренней стороны устройства заграждения, например, на внутренней стороне неметаллической двери, если её толщина не превышает 10 см.

При монтаже считывателя на металле рекомендуется, чтобы между основанием считывателя и металлической поверхностью расстояние было не менее 25 мм. В случае, когда стена, за которой установлен считыватель, оказывается слишком толстой или изготовлена из металла (содержит металлическую арматуру), считыватель допускается устанавливать на расстоянии, на котором должна быть обеспечена необходимая защита от возможного несанкционированного прохода.

Считыватели магнитных, Виганд карточек, электронных ключей и клавиатуры также рекомендуется размещать на стене или непосредственно на устройстве заграждения на высоте, удобной для пользования.

Считыватели магнитных карточек (за исключением совмещённых с исполнительными устройствами) во избежание помех или даже выхода из строя не рекомендуется устанавливать в непосредственной близости от мощных исполнительных устройств, создающих сильные электромагнитные поля (соленоидные, магнитные замки и т.п.).

Электромагнитные защёлки рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери, при закрывании двери и разблокировать замок при подаче сигнала от контроллера. Кроме того, такая установка защёлки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромеханические замки рекомендуется устанавливать на деревянных и металлических дверях массой до 100 кг при условии средней загруженности (до 100 – 200 проходов в день). Применение этих замков для дверей с высокой загруженностью неэффективно по причине высокого механического износа и, как следствие, снижения надёжности и срока службы. Чаще всего электромеханические замки устанавливают на двери (накладной или врезной замок), но иногда эти замки устанавливаются и на дверной коробке.

Электромагнитные замки рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг в условиях высокой загруженности (более 200 проходов в день). Отсутствие деталей, подверженных трению и износу, делает этот замок практически вечным. Особенностью данного замка является необходимость постоянной подачи тока на обмотку его электромагнита, так как при пропадании напряжения питания, например, при аварии или умышленном обрыве проводов, замок открывается. В связи с этим для надёжной работы необходимо дублирование его механическим замком или применение дополнительного резервного электропитания.

При совместном использовании магнитоконтактных извещателей в качестве датчиков положения двери с электромагнитными и электромеханическими замками, они должны быть разнесены друг от друга как можно дальше.

При установке исполнительных устройств (замки, доводчики, приводы и т.п.), требующих для своей работы подводки электропитания, необходимо использовать специальные устройства и кабели, обеспечивающие электро- и пожаробезопасность (особенно на сгораемых конструкциях), а также защиту от повреждений при открытии/закрытии дверей (гибкие переходы).

3.8 Общие требования к минимально необходимому составу СКУД.

3.8.1 Минимально необходимый состав СКУД.

Объекты органов внутренних дел Российской Федерации, отнесённые к четвертой категории, должны быть оборудованы СКУД.

СКУД оборудуются специальные помещения объекта.

Все входы в специальные помещения оборудуются замковыми устройствами и средствами охранной сигнализации, которые выдают сигнал тревоги при попытке преодоления нарушителем этих конструкций путём их вскрытия и разрушения.

3.8.2 Технические требования к СКУД.

СКУД должна обеспечивать:

– контроль и управление точками доступа (двери) на вход и выход;

– подключение считывателей электронных кодовых ключей;

– контроль аварийного открывания преграждающих устройств;

– контроль блокировки преграждающих устройств;

– контроль отказа от прохода;

– контроль исправности запорного устройства;

– возможность передачи тревожной информации на автоматизированные рабочие места системы сбора и обработки информации;

– контроль состояния связи с контроллерами системы контроля и управления доступом;

– защиту цепей питания от перенапряжения, переполюсовки и перегрузок;

– защиту входных цепей от перенапряжения и переполюсовки;

– предоставление доступа и идентификацию пользователей, проходящих через точку доступа по электронному ключу или электронной идентификационной карте;

– дистанционное управление (блокирование, разблокирование);

– автономную работу без потери данных в течение не менее 24 ч. при потере связи с автоматизированными рабочими местами;

– глобальный контроль повторного прохода;

– зональный контроль местоположения персонала;

– ведение журнала событий;

– получение отчёта о проходах;

– возможность наращивания количества устройств в процессе эксплуатации;

– идентификацию входящих (выходящих) по электронному ключу-идентификатору;

– идентификация (получение разрешения на проход, проезд) должна осуществляться по одному признаку.

Эвакуационные и аварийные выходы должны быть оборудованы устройством экстренного открывания дверей (устройство «Антипаника») по ГОСТ 31471-2011 «Устройства экстренного открывания дверей эвакуационных и аварийных выходов. Технические условия».

«Антипаниковая» дверь – это металлическая дверь, устойчивая к взлому снаружи и оборудованная специальными «антипаниковыми» замками и извещателем на открывание.

ПРИЛОЖЕНИЯ

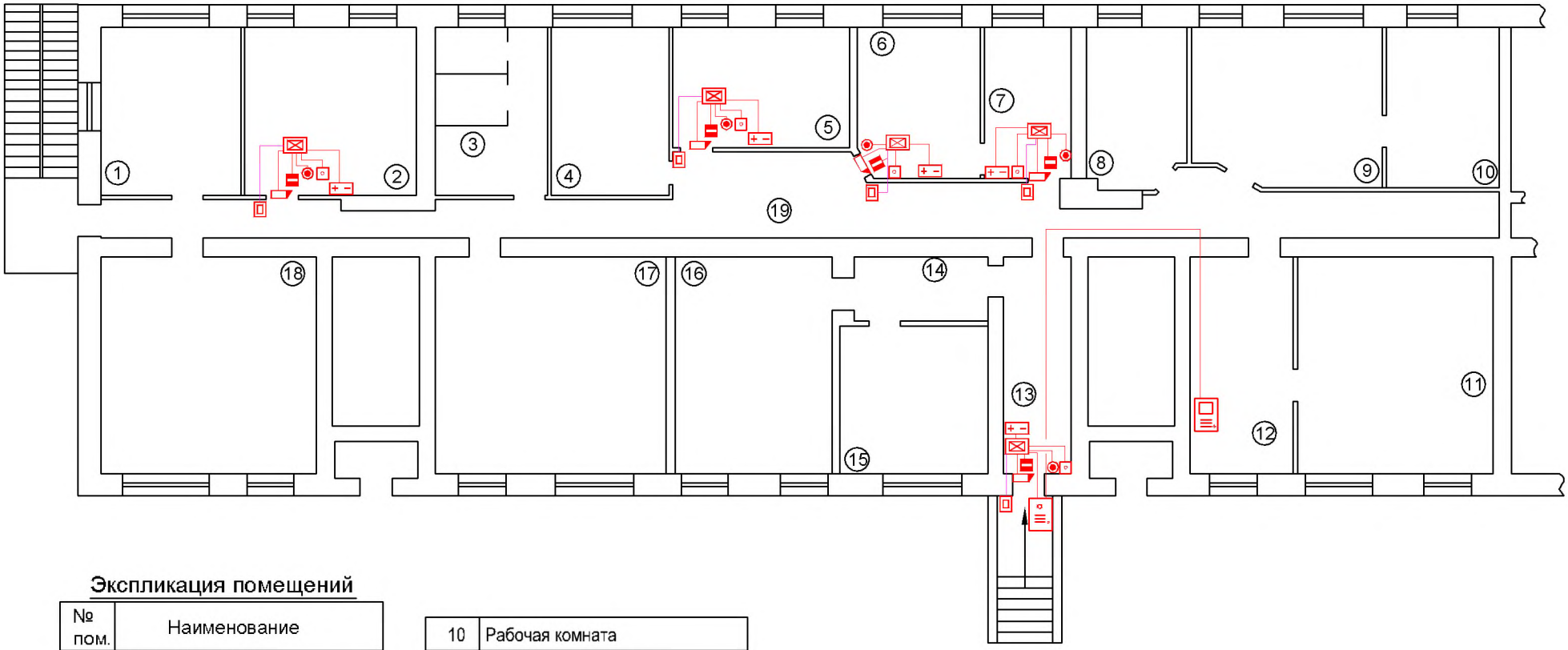
Приложение 1

Условные обозначения

Наименование	Обозначение	
	на планах	на схемах
Контроллер управления доступом		
Бесконтактный считыватель с клавиатурой		
Извещатель охранный магнитоконтактный		
Кнопка "ВЫХОД"		
Кнопка аварийного разблокировки электромагнитного замка (турникета)		
Электромагнитный замок		
Монитор видеодомофона		
Вызывная панель видеодомофона		
Резервированный источник электропитания питания 12В		
Провод КПСВВнг(А)FRLS1х2х0,5		
Провод FRLS4х2х0,5		

Приложение 2

План расположения оборудования СКУД в помещении ПЦО.



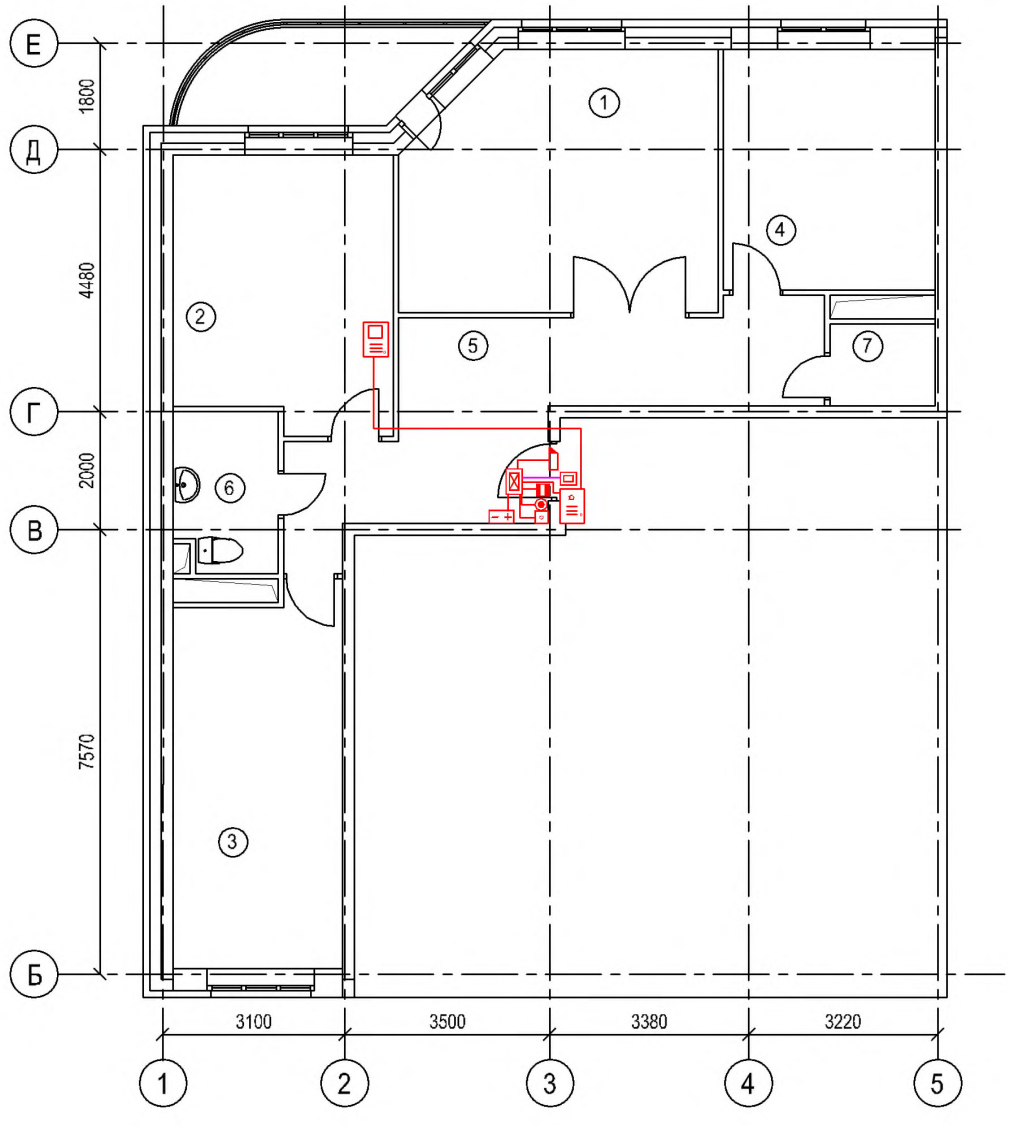
Экспликация помещений

№ пом.	Наименование
1	Рабочая комната
2	Спецпомещение
3	Туалет
4	Комната отдыха
5	ПЦО
6	ПЦО
7	Серверная
8	Рабочая комната
9	Рабочая комната

10	Рабочая комната
11	Кабинет начальника
12	Секретарь
13	Холл
14	Коридор
15	Квартирная группа
16	Бухгалтерия
17	Рабочая комноата
18	Кабинет заместителя начальника
19	Коридор

Приложение 3

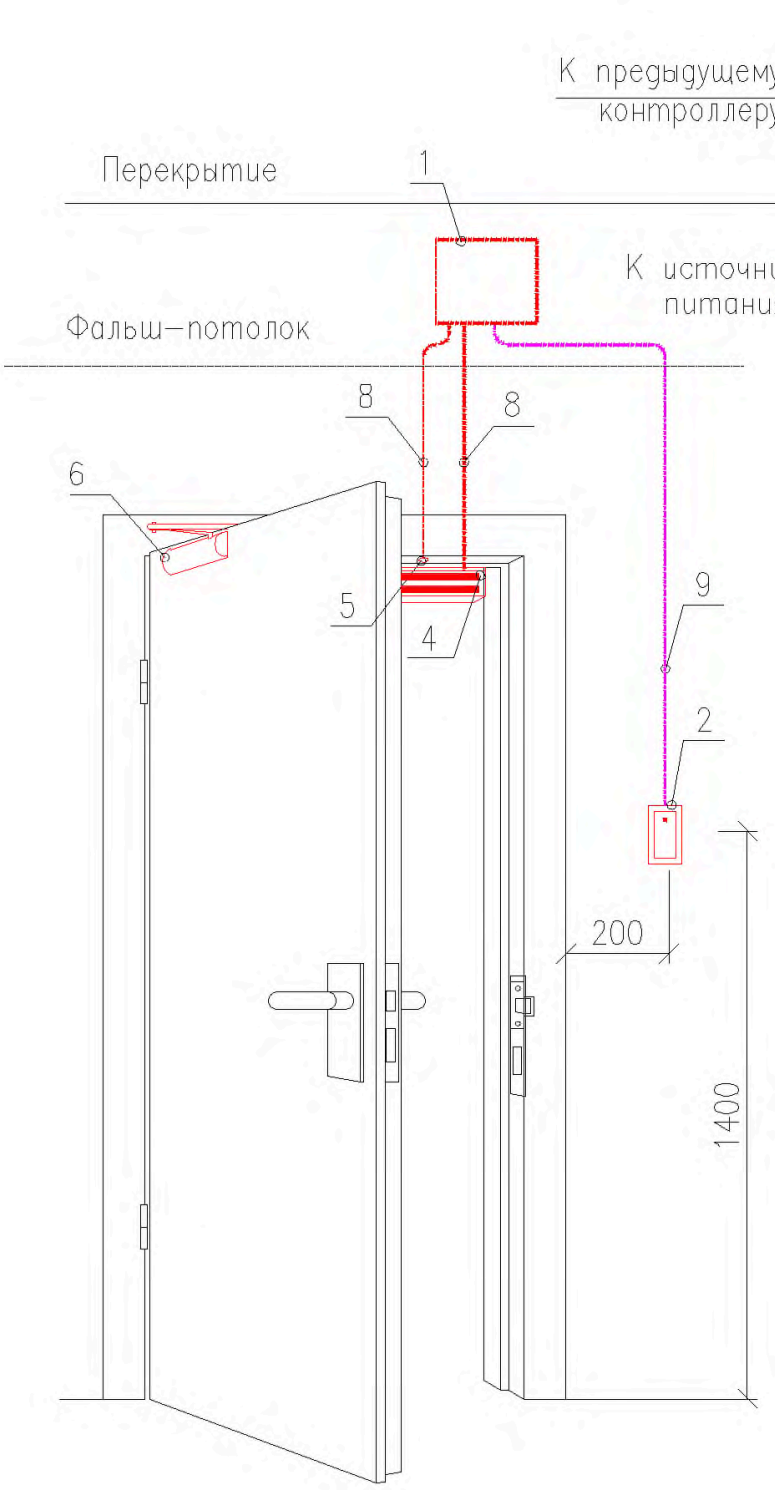
План расположения оборудования СКУД в помещении опорного пункта полиции.



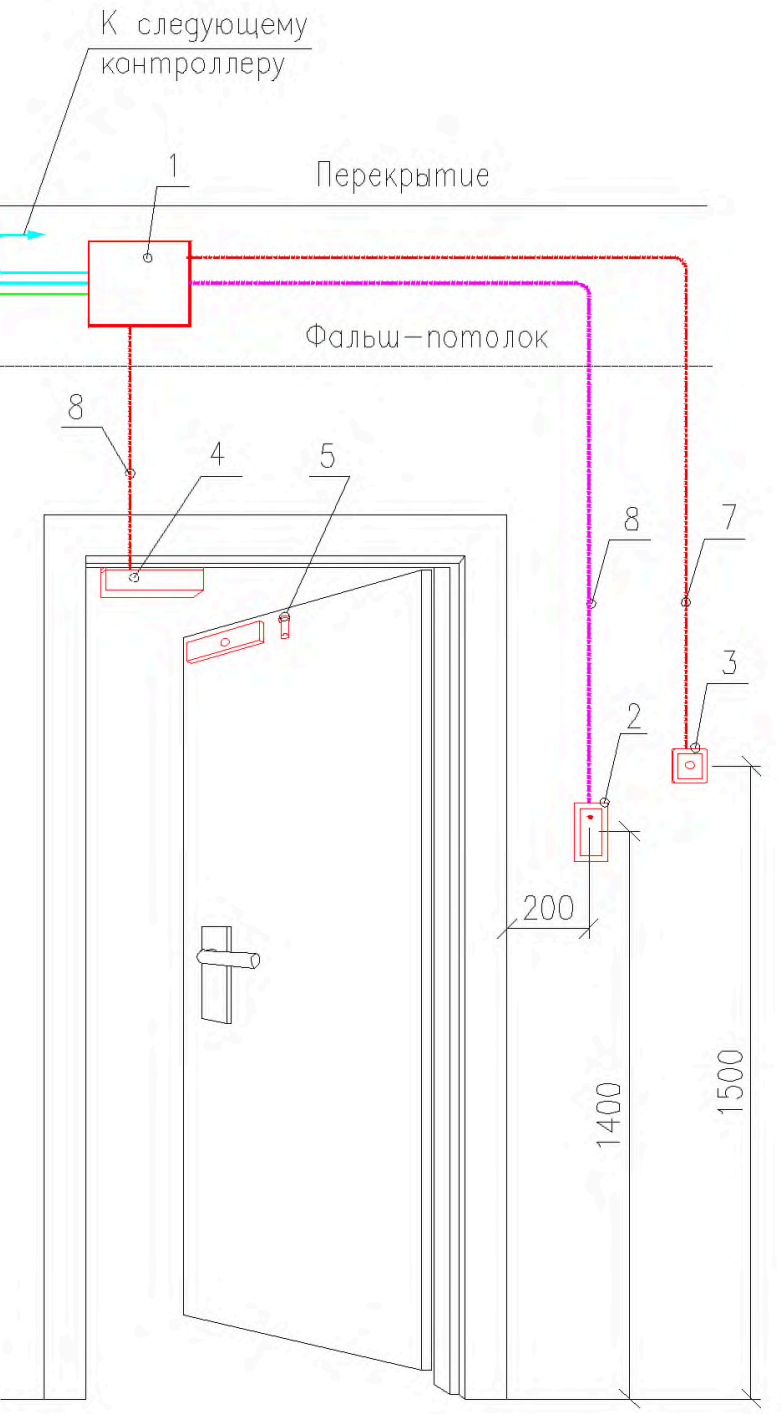
Экспликация помещений

№ пом.	Наименование	Площадь м^2
1	Рабочая комната	22,8
2	Рабочая комната	17,1
3	Рабочая комната	18,3
4	Рабочая комната	14,8
5	Холл	20,3
6	Санузел	4,7
7	Кладовая	2,3

Схемы установки средств СКУД на одностворчатой двери



Вид со стороны коридора



Вид со стороны защищаемого помещения

NN n/n	Наименование
1	Контроллер управления доступом
2	Бесконтактный считыватель с клавиатурой
3	Кнопка аварийной разблокировки электромагнитного замка
4	Электромагнитный замок
5	Извещатель охранный магнитоконтактный
6	Доводчик дверной
7	Провод
8	Провод

gost.e-ecolog.ru