Министерство внутренних дел Российской Федерации
Департамент государственной защиты имущества

«У Т В Е Р Ж Д А Ю»
Начальник ДГЗИ МВД России
генерал-лейтенант милиции

В.В. Савичев

«_____» _____ 20___ года

ВЫБОР И ПРИМЕНЕНИЕ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Р 78.36.005-2011

Рекомендации

МОСКВА 2011

В рекомендациях рассмотрены характеристики компонентов систем контроля и управления доступом, приведена их классификация, освещены вопросы обследования объектов, выбора систем контроля и управления доступом и их компонентов, особенностей размещения и монтажа.

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

СОДЕРЖАНИЕ

7. РАЗМЕЩЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ СКУД на ОБЪЕКТЕ

7.1. Устройства центрального управления

7.2. Устройства контроля управления

7.3. Считыватели и устройства исполнительные

8. МОНТАЖ ЭЛЕКТРОПРОВОДОК ТЕХНИЧЕСКИХ СРЕДСТВ СКУД на ОБЪЕКТЕ

8.1. Электропроводки технических средств СКУД

8.2. Монтаж линий связи, низковольтных цепей питания

8.3. Прокладка электропроводок в трубах

8.4. Прокладка электропроводок в коробах

8.5. Прокладка электропроводок напряжением 220 В

8.6. Монтаж электропроводок на территории объекта

ВВЕДЕНИЕ

В последние годы одним из наиболее эффективных подходов к решению задачи комплексной безопасности объектов различных форм собственности является использование систем контроля и управления доступом (СКУД). Правильное использование СКУД позволяет недопустить несанкционированный доступ на территорию, в здание, отдельные этажи и помещения. В то же время они не создают препятствий для прохода персонала и посетителей в разрешенные для них зоны. Интерес к СКУД неуклонно растет, что в недалеком будущем приведет к их широкому распространению. Следует помнить, что СКУД не устраняет необходимость контроля со стороны человека, но значительно повышает эффективность работы службы безопасности, особенно при наличии многочисленных зон риска. СКУД освобождает охранников от рутинной работы по идентификации, предоставляя им дополнительное время по выполнению основных функций: охране объекта и защите сотрудников и посетителей от преступных посягательств. Оптимальное соотношение людских и технических ресурсов выбирается в соответствии с поставленными задачами и допустимым уровнем возможных угроз.

Однако в настоящее время процесс выбора подходящих СКУД для решения конкретных задач носит сложный характер, поскольку реально отсутствует какая-либо аналитическая информация по имеющимся сегодня в мире СКУД. Некоторые компании, порой проявляют недобросовестность в рекламе, в предоставлении полной информации о технических и функциональных возможностях систем, об особенностях их эксплуатации в сравнительно сложных климатических условиях и т.п. Зачастую поставщики и продавцы ради прибыли предлагают заказчику аппаратуру низкого качества и неквалифицированные услуги. Повсеместно и сами покупатели не имеют достаточного опыта в этой сфере. В результате на важных объектах можно встретить непрофессионально спроектированные системы СКУД, у

которых даже технические характеристики не соответствуют условиям эксплуатации в России.

Целью настоящих рекомендаций является оказание помощи подразделениям вневедомственной охраны и ФГУП «Охрана» МВД России и специалистам служб безопасности различных организаций в правильном выборе структур и отдельных компонентов СКУД для конкретных объектов.

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящих Рекомендациях применяют следующие термины с соответствующими определениями.

1.1. **Аутентификация** - процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта.

1.2 **Биометрическая идентификация** - идентификация, основанная на использовании индивидуальных физических признаков человека.

1.3 **Вещественный код** - код, записанный на физическом носителе (идентификаторе).

1.4 **Взлом** - действия, направленные на несанкционированное разрушение конструкции.

1.5 **Временной интервал доступа (окно времени)** - временной интервал, в течение которого в данной точке доступа устанавливается заданный режим доступа.

1.6 **Вскрытие** - действия, направленные на несанкционированное проникновение через устройства преграждающие управляемые (УПУ), без его разрушения.

1.7 **Доступ** - перемещение людей (субъектов доступа), транспорта и других объектов (объектов доступа) в (из) помещения, здания, зоны и территории.

1.8 **Запоминаемый код –** код или кодовое слово (пароль), вводимый вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.

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

1.10 **Идентификатор доступа, идентификатор (носитель идентификационного признака) -** уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код – предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и другие подобные устройства).

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

1.12 **Контроллер доступа (КД), прибор приемно-контрольный доступа (ППКД) -** аппаратное устройство в составе средств управления СКУД.

1.13 **Контроль и управление доступом (КУД) -** комплекс мероприятий, направленных на предотвращения несанкционированного доступа.

1.14 **Копирование -** действия, производимые с идентификаторами, целью которых является получение копии идентификатора с действующим кодом.

1.15 **Криминальная безопасность -** состояние объекта защиты, при котором отсутствует недопустимый риск, связанный с причинением ему вреда от реализации криминальной угрозы.

1.16 **Манипулирование** - действия, производимые с устройствами контроля доступа, находящимися в рабочем режиме, без их разрушения, целью которых является получение действующего кода или приведение в открытое состояние УПУ. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него; следы такого действия не будут заметны. Манипулирование включает в себя также действия над программным обеспечением и действия по съему информации с каналов связи и интерфейсов устройств доступа.

1.17 **Наблюдение** - действия, производимые с устройствами контроля и управления доступом без прямого доступа к ним, целью которых является получение действующего кода.

1.18 **Несанкционированные действия (НСД)** - действия, целью которых является несанкционированное проникновение в зону доступа через УПУ.

1.19 **Несанкционированный доступ** - доступ субъектов или объектов, не имеющих права доступа.

1.20 **Пользователь СКУД** - субъект в отношении, которого осуществляются мероприятия по контролю доступа.

1.21 **Правило двух (и более) лиц** - правило доступа, при котором доступ разрешен только при одновременном присутствии двух или более лиц.

1.22 **Принуждение** - насильственные действия над лицом, имеющим право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.

1.23 **Пропускная способность** - способность средства или системы КУД пропускать через заданную точку доступа определенное количество субъектов или объектов доступа в единицу времени.

1.24 **Противокриминальная защита объектов и имущества** - деятельность, осуществляемая с целью обеспечения криминальной безопасности.

1.25 **Пулестойкость -** способность преграды противостоять сквозному пробиванию пулями и отсутствие при этом опасных для человека вторичных поражающих элементов.

1.26 **Саботаж -** преднамеренно созданное состояние системы или ее компонентов, при котором нарушается работоспособность, ухудшаются параметры, происходит повреждение системы.

1.27 **Санкционированный доступ -** доступ субъектов или объектов, имеющих права доступа.

1.28 **Система контроля и управления доступом (СКУД) -** совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

1.29 **Средства управления (СУ) -** аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации.

1.30 **Средства контроля и управления доступом (средства КУД) -** механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом.

1.31 **Точка доступа -** место, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода, оборудованные необходимыми средствами).

1.32 **Уровень доступа -** совокупность временных интервалов доступа (окон времени) и точек доступа, которые назначаются определенному лицу или группе лиц, имеющим доступ в заданные точки доступа в заданные временные интервалы.

1.33 **Устойчивость к взлому -** способность конструкции противостоять разрушающему воздействию.

1.34 **Устойчивость к взрыву -** способность конструкции противостоять разрушающему действию взрывчатых веществ.

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

1.36 **Устройства исполнительные (УИ) -** устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические, электромагнитные замки, электромагнитные защелки, механизмы привода шлюзов, ворот, турникетов и другие подобные устройства).

1.37 **Устройство считывающее (УС), считыватель -** устройство, предназначенное для считывания (ввода) идентификационных признаков.

2. ПРИНЦИП ДЕЙСТВИЯ СКУД

2.1. Основные принципы

В основе работы СКУД заложен принцип сравнения тех или иных **идентификационных признаков**, принадлежащих или присущих конкретному субъекту (физическому лицу) или объекту (предмету, транспортному средству), с информацией, заложенной в памяти системы.

Каждый из пользователей (сотрудников) получает индивидуальный идентификатор. Это может быть пароль или кодовое число, которые необходимо запомнить, или некоторый предмет, в который или на который, с помощью специальной технологии занесена кодовая информация.

В качестве такого предмета может быть использована пластиковая карта, брелок, браслет или другой подобный предмет. Идентификатор может быть закреплен также на определенном предмете и транспортном средстве.

Пароль, кодовое число, а также предмет-идентификатор относятся к классу **присвоенных** идентификационных признаков. При этом идентифицируется не сам человек, а присвоенный ему признак.

В качестве идентификационных признаков могут использоваться присущие признаки человека (биометрические данные) такие, как отпечатки пальцев, геометрия кисти руки, голосовые характеристики и т.д.). Биометрическая идентификация определяет человека по его **собственным** идентификационным признакам.

Работа СКУД происходит следующим образом. У входа в контролируемое помещение устанавливаются специальные устройства-считыватели, которые предназначены для считывания информации с идентификатора, ввода пароля или кодового числа, ввода биометрических данных человека. Далее информация поступает на **контроллеры доступа,** которые на основании анализа данных о владельце реагирует соответствующим образом, и обеспечивают управление **преграждающими и исполнительными устройствами**: открывает или блокирует дверь, включает сигнал тревоги, регистрирует присутствие человека на рабочем месте и т.д.

Понятие **идентификатора и идентификации** является основным понятием для СКД. Термин **идентификация** означает - опознавание, поиск по признаку. Идентификация может производиться по следующим основным принципам:

- **идентификация по запоминаемому коду** - по коду, вводимому вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств;
- **идентификация по вещественному коду** - по коду, записанному на физическом носителе (идентификаторе) в качестве которого применяются различные ключи, карты, брелоки и т.д.;

- **биометрическая идентификация** - идентификация, основанная на определении индивидуальных физических признаков человека.

2.1. Идентификация по запоминаемому коду

В качестве считывателей в этом случае используется цифровая или алфавитно-цифровая клавиатура, а также различные кодовые переключатели, панели или другие подобные устройства. Код вводится вручную, путем набора соответствующих символов или установки позиций переключателей. Название этого типа идентификации говорит о том, что код или пароль должен быть запомнен пользователем. Положительной стороной этого является то, что нет материального носителя кода, и соответственно не требуется затрат на его использование. Однако запоминание кода или пароля человеком имеет определенные недостатки. Для надежности код или пароль должен иметь как можно большее количество знаков. Например, по стандарту на СКУД, пароль доступа к программе компьютера должен иметь не менее шести знаков. Коды доступа для некоторых сейфовых замков высокой секретности имеют 12 знаков. Запомнить такое количество цифр или знаков для большинства людей достаточно трудно. Это приводит к тому, что зачастую код записывают на бумаге и хранят ее рядом с компьютером или с сейфом. При этом секретность доступа практически теряется. Еще одна проблема связана с проходными на крупных предприятиях. При большом потоке людей через проходную, ошибки, связанные с неправильным набором кода, резко снижают пропускную способность и порождают множество конфликтов со службой охраны.

Клавиатурные считыватели недостаточно защищены от манипуляций (подбор кода, наблюдение). Однако они имеют определенные достоинства, например разрядность кода, может быть выбрана произвольно, код может устанавливаться самим пользователем и произвольно им изменяться, и быть неизвестным оператору системы, также имеется возможность ввода

дополнительных кодов, например, кода «тихой» тревоги при нападении, кодов управления.

В настоящее время идентификация по запоминаемому коду применяется в простых автономных устройствах доступа или в качестве дополнительной наряду с другими видами.

2.2. Идентификация по вещественному коду

В настоящее время наибольшее распространение получили СКУД, использующие идентификацию по вещественному коду. Широкое распространение этот вид идентификации получил в связи с тем, что традиционно, для идентификации человека (удостоверения его личности) используется пропуск или другой документ – предмет на котором нанесена информация о человеке в виде его фотографии и соответствующих записей.

Собственно идентификация (опознавание) человека проводится также человеком (дежурным на проходной, охранником и т.д.) в основном по фотографии на документе. Здесь в полной мере свою отрицательную роль играет человеческий фактор. Состояние человека, усталость, потеря внимания, недостаточная бдительность и т.д. приводят к снижению надежности охраны.

В электронных автоматических системах в качестве идентификаторов используются пластиковые карты, брелоки, браслеты, механические или электронные ключи, и другие подобные устройства. В последние время пластиковые карты стали широко применяться в различных автоматизированных системах, в том числе и для контроля доступа. На пластиковые карты могут быть нанесены различные надписи, а также фотографии владельцев с помощью специальных принтеров или путем наклейки пленок. При этом карта доступа может служить и в качестве традиционного обычного документа.

Технология кодирования пластиковых карт отличается большим разнообразием – от простых и дешевых карт со штриховым кодом до карт с

электронной начинкой. Постоянно появляются новые типы пластиковых карт, использующие различные технологии, с целью повышения надежности, секретности кода и улучшения других характеристик.

2.3. Биометрическая идентификация

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 распространенные признаки человека, которые используются для биометрической идентификации:

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

Кроме того, в настоящее время ведутся разработки новых биометрических систем, использующих другие принципы действия, например, динамику клавиатурного почерка человека, изображение лица в инфракрасном свете и др.

Еще одним принципиальным отличием биометрического типа идентификации является вероятностный характер опознавания. При этом всегда присутствуют ошибки двух типов: вероятность несанкционированного допуска (ошибка первого рода) и вероятность ложного задержания (ошибка второго рода).

Однако в настоящее время величина этих ошибок для лучших устройств биометрической идентификации составляет: для ошибки первого рода – 0.0001%; для ошибки второго рода – 0.1%.

Такие характеристики позволяют 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.

2.4. Основные функции СКУД

В процессе своей работы 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.).

Процедура санкционирования производится оператором или администратором системы и заключается во вводе необходимых данных в

компьютер системы или в память контроллера. Все остальные процедуры могут производиться системой автоматически. Очевидно, что процедура аутентификации может быть выполнена полноценно только с помощью биометрических систем.

3. КЛАССИФИКАЦИЯ СРЕДСТВ И СИСТЕМ КУД

3.1. Классификация средств КУД

3.1.1. Средства КУД классифицируются по:

- функциональному назначению устройств;
- функциональным характеристикам;
- устойчивости к НСД.

3.1.2. Средства КУД по функциональному назначению устройств подразделяются на следующие основные средства:

- устройства преграждающие управляемые (УПУ);
- устройства исполнительные (УИ);
- устройства считывающие (УС);
- идентификаторы (ИД);
- средства управления (СУ) в составе аппаратных устройств и программных средств.

В состав СКУД могут входить другие дополнительные средства: источники электропитания; датчики (извещатели) состояния УПУ; дверные доводчики; световые и звуковые оповещатели; кнопки ручного управления УПУ; устройства преобразования интерфейсов сетей связи; аппаратура передачи данных по различным каналам связи и другие устройства, предназначенные для обеспечения работы СКУД.

В состав СКУД могут входить также аппаратно-программные средства – средства вычислительной техники (СВТ) общего назначения (компьютерное оборудование, оборудование для компьютерных сетей, общее программное обеспечение).

3.1.3. Средства КУД по функциональным характеристикам классифицируются на следующие группы.

3.1.3.1. УПУ классифицируются по виду перекрытия проема прохода.

По виду перекрытия проема прохода УПУ могут быть:

- с частичным перекрытием (турникеты, шлагбаумы);
- с полным перекрытием (полноростовые турникеты, специализированные ворота);
- со сплошным перекрытием проема (сплошные двери, ворота);
- с блокированием объекта в проеме (шлюзы, кабины проходные).

3.1.3.2. УИ классифицируются по способу запирания:

- электромеханические замки;
- электромагнитные замки;
- электромагнитные защелки;
- механизмы привода дверей, ворот.

3.1.3.3. Идентификаторы и считыватели классифицируются по следующим признакам:

- по виду используемых идентификационных признаков (идентификаторы и считыватели);
- по способу считывания идентификационных признаков (считыватели).

По виду используемых идентификационных признаков идентификаторы и считыватели могут быть:

- механические - идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
- магнитные - идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда, и т.д.);

- оптические - идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т.д.);
- электронные контактные - идентификационные признаки представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т.д.);
- электронные радиочастотные идентификаторы, считывание кода с которых происходит путем передачи данных по радиоканалу;
- акустические - идентификационные признаки представляют собой кодированный акустический сигнал;
- биометрические (только для считывателей) - идентификационные признаки представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т.д.);
- комбинированные - для идентификации используются одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков считыватели могут быть:

- с ручным вводом - ввод производится с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;
- контактные - ввод происходит при непосредственном, в том числе и при электрическом, контакте между считывателем и идентификатором;
- бесконтактные - считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю;
- комбинированные.

3.1.3.4. Классификация средств управления СКУД включает в себя:

- аппаратные средства (устройства) – контроллеры доступа (приборы приемно-контрольные доступа);
- программные средства – программное обеспечение СКУД;

3.2. Классификация систем КУД

3.2.1. Системы КУД классифицируются по:

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

3.2.2. По способу управления системы КУД могут быть:

- автономные - для управления одним или несколькими 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.

3.2.3. По количеству контролируемых точек доступа:

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

3.2.4. По функциональным характеристикам системы КУД могут быть трех классов:

1. системы с ограниченными функциями;
2. системы с расширенными функциями;
3. многофункциональные системы.

3.3. Классификация средств и систем КУД по устойчивости к НСД

3.3.1. Классификация средств КУД по устойчивости к НСД определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости:

- нормальной;
- повышенной;
- высокой.

3.3.2. 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.

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

3.3.4. 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.

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

3.4. Условные обозначения средств и систем КУД

3.4.1. Условные обозначения средств КУД содержат:

а) название или обозначение устройства (средства) в соответствии с таблицей 1;

Таблица 1. Название и обозначение средств СКУД

Название	Обозначение
Устройство преграждающее управляемое	УПУ
Устройство исполнительное	УИ
Устройство считывающее (считыватель)	УС
Идентификатор	ИД
Средства управления - аппаратные устройства:	

контроллер доступа; прибор приемно-контрольный доступа	КД ППКД
Средства управления – программные: программное обеспечение	ПО

б) аббревиатуру СКУД;

в) группы символов: $X_1X_2 – X_3/X_4X_5$, где:

X_1 - классификация по функциональным характеристикам в соответствии с Таблицей 2;

Таблица 2. Обозначение классификации по функциональным характеристикам средств СКУД

Средства КУД по функциональному назначению	Классификация по функциональным характеристикам	Обозначение
Устройства преграждающие управляемые (УПУ) X1 – по виду перекрытия прохода	С частичным перекрытием (турникеты, шлагбаумы)	1
	С полным перекрытием (полноростовые турникеты, специализированные ворота)	2
	Со сплошным перекрытием проема (сплошные двери, ворота)	3
	С блокированием объекта в проеме (шлюзы, кабины проходные)	4
Устройства исполнительные (УИ) X1 – по способу запирания	Электромеханические замки	1
	Электромагнитные замки	2
	Электромагнитные защелки	3
	Механизмы привода ворот	4
Устройства считывающие (УС) X1 – по способу	С ручным вводом	1
	Контактные	2
	Бесконтактные	3

считывания идентификационных признаков	Биометрические	4
	Комбинированные	5
Идентификаторы (ИД) Х1 – по виду идентификационных признаков	Механические	1
	Магнитные	2
	Оптические	3
	Электронные контактные	4
	Электронные радиочастотные	5
	Акустические	6
	Комбинированные	7
Контроллер доступа (КД), прибор приемно-контрольный доступа (ППКД) Х1- по способу управления	Автономный	1
	Централизованный	2
	Универсальный	3

X_2 - уровень устойчивости к НСД (Н – нормальный, П – повышенный, В – высокий);

X_3 - порядковый номер разработки средства КУД (порядковый номер X_3 регистрируется соответствующим государственным органом, ответственным за проведение технической политики в данной сфере).

X_4 – обозначение конструктивного исполнения;

X_5 – обозначение модернизации, русская прописная буква в алфавитном порядке (первая модернизация – А, вторая – Б и т.д.);

г) обозначение технических условий (ТУ).

Примеры условного обозначения.

Идентификатор КУД электронный радиочастотный, нормальной устойчивости к НСД, порядковый номером разработки 5, конструктивное исполнение 8, модификация А:

ИД СКУД 5Н – 5/8А ТУ ХХ ХХХХ ХХХХ

3.4.2. Условное обозначение систем КУД состоит из:

а) названия «Система контроля и управления доступом» или сокращенно СКУД;

в) группы символов: $X_1\ X_2\ X_3\ X_4 – X_5 / X_6\ X_7$, где:

X_1 – способ управления:

- 1 – автономная;

- 2 – централизованная (сетевая);

- 3 – универсальная (сетевая);

X_2 – количество контролируемых точек доступа:

- 1 – малой емкости;

- 2 – средней емкости ;

- 3 – большой емкости;

X_3 – класс по функциональным характеристикам:

X_4 – класс защищенности системы от несанкционированного доступа к информации для систем повышенной и высокой устойчивости к НСД или буква «Н» для систем нормальной устойчивости;

X_5 – порядковый номер разработки (порядковый номер X_5 регистрируется соответствующим государственным органом, ответственным за проведение технической политики в данной сфере);

X_6 – обозначение конструктивного исполнения;

X_7 – обозначение модернизации (обозначается русской прописной буквой в алфавитном порядке, первая модернизация – А, вторая – Б и т.д.)

д) обозначение технических условий (ТУ)

Примеры условного обозначения.

Система контроля и управления доступом сетевая, малой емкости, второго класса по функциональным возможностям, нормальной устойчивости к НСД, номер разработки 7, конструктивное исполнение 9, модернизация – Б:

СКУД – 212Н-7/9Б ТУ ХХ ХХХХ ХХХХ.

4. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

4.1. Общие требования

4.1.1. Средства и системы КУД должны обеспечивать возможность непрерывной работы, с учетом проведения регламентного технического обслуживания.

4.1.2. Системы КУД в основном рабочем режиме должны обеспечивать автоматическую работу. Режим ручного или автоматизированного управления (с участием оператора) должен обеспечиваться только при возникновении чрезвычайных, аварийных или тревожных ситуаций, а также по требованию заказчика.

4.1.3. Средства и системы КУД в системах противокриминальной защиты объектов должны обеспечивать:

- защиту от несанкционированного доступа на охраняемый объект (помещение, зону) в режиме снятия их с охраны;
- контроль и учет доступа персонала (посетителей) на охраняемый объект (помещение, зону) в режиме снятия их с охраны;
- автоматизацию процессов взятия/снятия охраняемого объекта (помещения, зоны) с помощью средств идентификации СКУД в составе устройств и приборов охранной сигнализации;
- защиту и контроль доступа к компьютерам автоматизированных рабочих мест (АРМ) пультового оборудования систем охранной сигнализации.

4.2. Требования к функциональным характеристикам средств КУД

4.2.1. Требования к функциональным характеристикам УПУ и УИ

4.2.1.1. УПУ в закрытом состоянии должны обеспечивать физическое препятствие доступу в соответствии с классификацией по виду перекрытия проема:

- частичное перекрытие (турникеты, шлагбаумы);
- полное перекрытие (полноростовые турникеты, специализированные ворота);
- сплошное перекрытие проема (сплошные двери, сплошные ворота);
- блокирование объекта в проеме (шлюзы, кабины проходные).

4.2.1.2. УПУ в рабочем режиме могут быть двух типов:

- нормально открытые;
- нормально закрытые.

Нормально открытые УПУ должны быть оснащены датчиком приближения субъекта и объекта доступа, обеспечивать свободный проход при санкционированном доступе и переходить в закрытое состояние, если доступ несанкционирован.

Нормально закрытые УПУ должны открываться при санкционированном доступе.

4.2.1.3. УПУ с частичным перекрытием проема, при необходимости, должны быть оснащены средствами сигнализации, срабатывающими при попытке обхода преграждающего устройства.

4.2.1.4. УПУ при санкционированном доступе должны переходить в открытое состояние при подаче управляющего сигнала от устройства управления.

Нормально закрытые УПУ при необходимости, должны быть оборудованы средствами звуковой сигнализации, которая включается после их открывания и при отсутствии прохода в течение установленного времени, и должны иметь средства для возврата в закрытое состояние.

4.2.1.5. УПУ при необходимости должны иметь защиту от прохода через них одновременно двух или более человек.

4.2.1.6. УПУ должны иметь возможность механического аварийного открывания в случае пропадании электропитания, возникновения пожара или других чрезвычайных ситуаций. Аварийная система открывания должна быть

защищена от возможности использования ее для несанкционированного проникновения.

4.2.1.7. В конструкции УПУ должны быть предусмотрены меры по защите внешних электрических соединительных цепей от несанкционированных воздействий (подачи напряжений, обрыва, короткого замыкания), приводящих к открыванию УПУ.

4.2.1.8. УПУ могут иметь дополнительно средства специального контроля (металлодетекторы, обнаружители радиоактивных веществ и др.), встроенные или совместно функционирующие.

4.2.1.9. Устройства исполнительные должны обеспечивать приведение УПУ в закрытое или открытое состояние.

УИ могут быть самостоятельными изделиями или быть выполнены как часть конструкции УПУ.

4.2.2. Требования к функциональным характеристикам ИД и УС

4.2.2.1. Считыватели должны обеспечивать:

- ввод запоминаемого кода;
- считывание идентификационного признака с идентификаторов;
- введение биометрической информации (для считывателей биометрической информации);
- преобразование введенной информации в электрический сигнал;
- передачу информации на контроллер СКУД.

4.2.2.2. Считыватели должны иметь световую индикацию работоспособности и состояния доступа. Рекомендуемый режим работы:

- непрерывное свечение индикатора красного цвета – доступ закрыт;
- непрерывное свечение индикатора зеленого цвета – доступ открыт.

Допускается в режиме экономии электропитания световую индикацию работоспособности и состояния доступа отображать кратковременными вспышками соответствующего цвета.

При необходимости считыватели должны иметь звуковой сигнализатор. Параметры звуковых сигналов и события, которые они индицируют должны быть описаны в документации на изделия.

Допускается в считывателе не иметь индикации, в этом случае должно быть оговорено в документации, что эти считыватели должны использоваться с контроллерами СКУД, которые обеспечивают управление внешними световыми и звуковыми индикаторами.

4.2.2.3. Считыватели должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды и степень защиты должны быть указаны в стандартах и (или) нормативных документах на устройства конкретного типа. Информация, содержащаяся в документации не должна снижать степень защиты.

4.2.2.4. Считыватели при взломе и вскрытии, а также в случае обрыва или короткого замыкания, подходящих к ним цепей, не должны вызывать открытие УПУ. При этом автономные системы должны выдавать звуковой сигнал тревоги, а системы с централизованным управлением дополнительно должны передавать сигнал тревоги на пункт управления.

4.2.2.5. Идентификаторы должны иметь уникальный идентификационный признака (код, номер), который не должен повторяться. В случае если такое повторение возможно, в документации на изделия должны быть указаны условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами.

4.2.2.6. Идентификаторы должны обеспечивать хранение идентификационного признака в течение всего срока службы при эксплуатации.

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

4.2.3. Требования к функциональным характеристикам СУ

4.2.3.1. Аппаратные средства управления (контроллеры) должны обеспечивать прием информации от считывателей, обработку информации и выработку сигналов управления на исполнительные устройства.

4.2.3.2. Контроллеры в системах с централизованным управлением и универсальных должны обеспечивать:

- обмен информацией по линии связи между контроллерами и средствами централизованного управления;
- сохранность данных в памяти, при обрыве линий связи со средствами централизованного управления, отключении питания и при переходе на резервное питание;
- контроль линий связи между контроллерами, средствами централизованного управления.

Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также, при необходимости, имитостойкость и защиту информации (для систем повышенной и высокой устойчивости).

Виды и параметры протоколов и интерфейсов должны быть установлены в стандартах и других нормативных документах на контроллеры конкретного типа.

4.2.3.3. Контроллеры должны иметь входы для подключения цепей сигнализации состояния УПУ, кнопки запроса на выход, контакта вскрытия корпуса, контакта отрыва от стены. Контроллеры СКУД дополнительно могут иметь входы для подключения шлейфов охранной сигнализации.

4.2.3.4. Контроллеры должны иметь выходы для подключения цепей управления исполнительными устройствами, выходы управления световой индикацией состояния доступа по каждому направлению, выходы управления световой и звуковой индикацией тревожных состояний.

4.2.3.5. Сетевые СКУД должны иметь средства централизованного управления, в качестве которых могут использоваться СВТ общего назначения (персональные компьютеры) или специализированные компьютеры. Основным компонентом средств управления сетевых СКУД является программное обеспечение (ПО).

В комплект эксплуатационной документации сетевой СКУД должно входить «Руководство по эксплуатации программного обеспечения», в котором должны быть указаны требования к компьютеру и составу общесистемных программ, необходимых для работы ПО СКУД.

4.2.3.6. Программное обеспечение сетевых СКУД должно обеспечивать:

- эргономичный экранный интерфейс с пользователем (оператором СКУД);
- занесение кодов идентификаторов в память системы;
- задание характеристик точек доступа;
- установку временных интервалов доступа (окон времени);
- установку уровней доступа для пользователей;
- протоколирование текущих событий;
- протоколирование тревожных событий;
- ведение и поддержание баз данных;
- регистрацию прохода через точки доступа в протоколе базы данных;
- сохранение баз данных и системных параметров на резервном носителе;
- сохранение баз данных и системных параметров при авариях и сбоях в системе;
- приоритетный вывод информации о нарушениях;
- возможность управления УПУ в случае чрезвычайных ситуаций.

4.2.3.7. Программное обеспечение должно быть устойчиво к случайным и преднамеренным воздействиям следующего вида:

- отключение питания аппаратных средств;

- программный рестарт аппаратных средств;
- аппаратный рестарт аппаратных средств;
- случайное нажатие клавиш на клавиатуре;
- случайный перебор пунктов меню программы.

После указанных воздействий и перезапуске программы должна сохраняться работоспособность системы и сохранность установленных данных. Указанные воздействия не должны приводить к открыванию УПУ и изменению действующих кодов доступа.

4.3. Требования к функциональным характеристикам систем КУД

4.3.1. Автономные системы КУД должны обеспечивать:

- выдачу сигнала на открывание УПУ при считывании зарегистрированного в памяти системы идентификационного признака;
- запрет открывания УПУ при считывании незарегистрированного в памяти системы идентификационного признака;
- запись идентификационных признаков в память системы;
- защиту от несанкционированного доступа при записи кодов идентификационных признаков в памяти системы;
- сохранение идентификационных признаков в памяти системы при отказе и отключении электропитания;
- ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;
- автоматическое формирование сигнала закрытия на УПУ при отсутствии факта прохода;
- выдачу сигнала тревоги при аварийном открывании УПУ для несанкционированного проникновения.

4.3.2. Дополнительные характеристики автономных систем в зависимости от класса по функциональным характеристикам приведены в таблице 1.

В систему любого класса могут быть введены дополнительные характеристики.

Таблица 1. Функциональные характеристики автономных систем

Функциональные характеристики автономной системы		Классы		
		1	2	3
1	Установка уровней доступа	-	-	+
2	Установка временных интервалов доступа	-	+	+
3	Возможность регулирования времени открывания УИ	-	+	+
4	Возможность идентификации по двум признакам	-	-	+
5	Защита от повторного использования идентификатора для прохода в одном направлении	-	-	+
6	Ввод специального идентификационного признака для открывания под принуждением	-	-	+
7	Подключение считывателей различных типов	-	+	+
8	Доступ по «правилу двух (и более) лиц»	-	-	+
9	Световая индикация о состоянии доступа	+	+	+
10	Контроль состояния УПУ	-	+	+
11	Световое и/или звуковое оповещение о попытках НСД	-	-	+
12	Регистрация и хранение информации о событиях в энергонезависимой памяти	-	+	+
13	Количество событий, хранимых в энергонезависимой памяти, не менее	-	64	256
14	Ведение даты и времени возникновения событий	-	+	+
15	Возможность подключения устройства для вывода информации о событиях	-	+	+
16	Возможность передачи информации о событиях на ЭВМ	-	-	+
17	Возможность интегрирования с системой охранной сигнализации на релейном уровне	-	+	+

18	Возможность интегрирования с системой охранного телевидения на релейном уровне	-	-	+
Примечание. Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «-» - отсутствие функции.				

4.3.3. Системы КУД с централизованным управлением и универсальные должны соответствовать общим функциональным требованиям как для автономных систем и дополнительно обеспечивать:

- работу в локальной сети контроллеров СКУД под управлением компьютера с установленным на нем ПО СКУД;
- регистрацию и протоколирование тревожных и текущих событий;
- приоритетное отображение на экране управляющего компьютера тревожных событий;
- управление работой УПУ в точках доступа по командам оператора;
- задание временных режимов действия идентификаторов в точках доступа, и уровней доступа;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
- установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т.п.);
- блокировку прохода по точкам доступа командой с пункта управления в случае нападения;

- возможность подключения дополнительных средств специального контроля, средств досмотра.

4.3.4. Дополнительные характеристики систем с централизованным управлением, в зависимости от класса по функциональным характеристикам, приведены в таблице 2.

В систему любого класса могут быть введены дополнительные характеристики.

Таблица 2. Функциональные характеристики систем с централизованным управлением и универсальных

Функциональные характеристики систем с централизованным управлением (сетевых) и универсальных		Классы системы		
		1	2	3
1	Количество уровней доступа, не менее	16	64	256
2	Количество временных интервалов доступа, не менее	16	64	256
3	Защита от повторного использования идентификатора для прохода в одном направлении: - локальная; - глобальная.	 - -	 + -	 + +
4	Возможность двойной идентификации	-	+	+
5	Поддержка биометрической идентификации	-	-	+
6	Ввод специального идентификационного признака для открывания под принуждением	-	+	+
7	Подключение считывателей различных типов	-	+	+
8	Доступ по «правилу двух (и более) лиц»	-	+	+
9	Количество событий, сохраняемых в энергонезависимой памяти контроллеров, не менее	1000	5000	10000
10	Возможность интегрирования с системой охранной и пожарной сигнализации на релейном	+	-	-

	уровне			
11	Возможность интегрирования с системой видео контроля на релейном уровне	+	-	-
12	Возможность интегрирования с системой охранной, пожарной сигнализации и системами видеоконтроля на системном уровне	-	+	+
13	Возможность управления работой дополнительных устройств в точках доступа (освещение, вентиляции, лифты, технологическое оборудование и т.п.)	-	-	+
14	Обеспечение изображения на экране ЭВМ плана объекта и (или) помещений объекта с указанием мест расположения средств контроля доступа, охранной и пожарной сигнализации, средств видеоконтроля и графическим отображением тревожных состояний в контрольных точках на плане	-	+	+
15	Интерактивное управление средствами по изображению плана объекта на экране ЭВМ	-	-	+
16	Ведение баз данных на пользователей	-	+	+
17	Поддержание фотографических данных пользователей в базе данных	-	-	+
18	Контроль над перемещением и поиск пользователей	-	-	+
Примечание - Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «-» - отсутствие функции.				

4.3.5. Универсальные системы должны обеспечивать автономную работу при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи, а также восстановление режимов работы после устранения отказов и восстановлении связи.

4.3.6. Системы КУД должны также иметь следующие характеристики:

- максимальное количество точек доступа, зон доступа, пользователей, обслуживаемых системой;
- максимальное количество точек доступа, обслуживаемых одним контроллером;
- максимальное количество контроллеров в системе;
- количество считывателей на один контроллер системы;
- количество и вид временных интервалов доступа, уровней доступа;
- количество типов считывателей, используемых в системе;
- время реакции системы на заявку на проход;
- максимальная длина линии связи с контроллерами и допустимые параметры линии связи;
- максимальное расстояние действия считывателя (для бесконтактных считывателей);
- максимальное время хранения информации о событиях в памяти системы;
- максимальная пропускная способность для системы в точках доступа;
- вероятность несанкционированного доступа, вероятность ложного задержания (для СКУД с биометрической идентификацией);
- показатели по уровням устойчивости к НСД.

4.3.7. По требованиям заказчика допускается устанавливать дополнительные характеристики и показатели в технических условиях на системы конкретного типа.

4.4. Требования по устойчивости средств и систем КУД к НСД

4.4.1. Требования по устойчивости к НСД неразрушающего воздействия устанавливаются для средств КУД в зависимости от функционального назначения и включают:

- устойчивость к вскрытию для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивость к манипулированию;
- устойчивость к наблюдению для считывателей с запоминаемым кодом (клавиатуры, кодовые переключатели и т.п.);
- устойчивость к копированию идентификаторов.

Показатели устойчивости по данным требованиям и методы их испытаний должны быть установлены в стандартах и (или) технических условиях на средства КУД конкретного типа.

4.4.1. Программное обеспечение сетевых систем должно быть защищено от несанкционированного доступа. Требования по защите программного обеспечения систем КУД должны обеспечиваться средствами ограничения и администрирования доступа операционных систем управляющего компьютера СКУД и разграничением доступа к ПО СКУД. Рекомендуемые уровни защиты доступа к ПО с помощью паролей с разделением по типу пользователей:

- первый («администратор») - доступ ко всем функциям;
- второй («дежурный оператор») - доступ только к функциям текущего контроля;
- третий («системный оператор») - доступ к функциям конфигурации программного обеспечения без доступа к функциям, обеспечивающим управление УПУ.

Количество знаков в пароле должно быть не менее шести.

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

4.5. Требования к надежности

4.5.1. На средства и системы КУД конкретного типа устанавливают следующие показатели надежности:

- средняя наработка на отказ, ч;
- среднее время восстановления работоспособного состояния, ч;
- средний срок службы, лет.

При установлении показателей надежности должны быть указаны критерии отказа.

Показатели надежности средств КУД устанавливаются исходя из необходимости обеспечения надежности системы в целом.

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

4.5.2. Средняя наработка на отказ систем КУД на одну точку доступа (без учета УПУ) должна быть не менее 10000 ч.

4.5.3. Средний срок службы систем КУД должен быть не менее 8 лет с учетом проведения восстановительных работ.

4.6. Требования к электропитанию

4.6.1. Основное электропитание средств и систем КУД должно осуществляться от сети переменного тока частотой 50 Гц с номинальным напряжением 220 В.

Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения сети от минус 15 до +10 %.

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

4.6.2. Средства и системы КУД должны иметь резервное электропитание при пропадании напряжения основного источника питания. В качестве резервного источника питания может использоваться резервная сеть переменного тока или источники питания постоянного тока.

Номинальное напряжение резервного источника питания постоянного тока выбирается из ряда: 12, 24 В.

Переход на резервное питание должен происходить автоматически без нарушения установленных режимов работы и функционального состояния средств и систем КУД.

Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения резервного источника от минус 15 до плюс 10 % от номинального значения.

4.6.3. Резервный источник питания должен обеспечивать выполнение основных функций системы при пропадании напряжений в сети на время не менее 0,5 ч для систем первого и второго класса по функциональным характеристикам и не менее 1ч для систем третьего класса.

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

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

4.6.5. При использовании в качестве источника резервного питания аккумуляторных или сухих батарей, рекомендуется иметь индикацию разряда батареи ниже допустимого предела. Для автономных систем индикация разряда может быть световая или звуковая, для сетевых систем сигнал разряда батарей может передаваться на пункт управления.

4.6.6. Химические источники питания, встроенные в идентификаторы или обеспечивающие сохранность данных в контроллерах, должны обеспечивать работоспособность средств КУД в течение времени, не менее 3 лет.

4.7. Требования безопасности

4.7.1. Электрическое сопротивление изоляции средств и систем КУД между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должно быть не менее значений, указанных в таблице 5.

Таблица 5. Требуемые значения сопротивления изоляции

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

4.7.2. Средства и системы КУД, предназначенные для эксплуатации в зонах с взрывоопасной средой должны соответствовать требованиям нормативных документов, регламентирующих требования к изделиям, предназначенным для работы во взрывоопасных средах.

5. ВЫБОР СКУД ДЛЯ ОБОРУДОВАНИЯ ОБЪЕКТА

5.1. Обследование объекта

Выбор варианта оборудования объекта средствами СКУД следует начинать с его обследования. При обследовании определяются характеристики значимости помещений объекта, его строительные и архитектурно - планировочные решения, условия эксплуатации, режимы работы, ограничения или, наоборот, расширения права доступа отдельных сотрудников, параметры установленных (или предполагаемых к установке на данном объекте) средств, входящих в СКУД. 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 КУД;

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 КУД 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 КУД в аварийных и чрезвычайных ситуациях;
- программное обеспечение системы;
- требования к безопасности;
- требования к электропитанию;
- обслуживание и ремонт системы;
- требования к возможности включения системы КУД в интегрированную систему безопасности.

5.1.1. Архитектурно-планировочные и строительные решения

Путем 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.

5.1.2. Условия эксплуатации

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 (запыленность, повышенная влажность, отрицательная температура, агрессивная среда и т. п.). Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, удаленность считывателей и контроллеров от управляющего центра, заземление составных частей системы и т.п.

5.1.3. Интегрированные системы безопасности (ИСБ)

В настоящее время любой крупный и особенно важный объект имеет весь набор технических средств безопасности, включающий в себя системы ОПС, ТСВ, СКУД и д.р. Многообразие и разрозненность этих систем на одном объекте приводит к неэффективности их работы, трудностях в управлении и обслуживании. Объединение всех систем в единый программно-аппаратный комплекс (или другими словами создание ИСБ с общей информационной средой и единой базой данных) позволяет:

- минимизировать капитальные затраты на оснащение объекта. Аппаратная часть значительно сокращается как за счет

исключения дублирующей аппаратуры в разных системах, так и из-за увеличения эффективности работы каждой системы;

- на основе полной и объективной информации, поступающей оператору значительно сокращается время, необходимое на принятие соответствующих решений по пресечению несанкционированного проникновения, проходу и других чрезвычайных ситуаций на объекте;
- оптимизировать необходимое число постов охраны и существенно снизить расходы на их содержание, а также уменьшить влияние субъективного человеческого фактора;
- четко разграничить права доступа, как своих сотрудников, так и посторонних в охраняемые помещения и к получению информации;
- автоматизировать процессы взятия, снятия охраняемых помещений, включения телевизионных камер, контроля шлейфов охранно-пожарной сигнализации и т.п.

При создании ИСБ следует учитывать:

- возможность совместной синхронизации всех составляющих ИСБ устройств;
- возможность интеграции на программном, аппаратном и релейных уровнях;
- возможность организации линий связи стандартных интерфейсов (при значительной удаленности панелей систем сигнализации и управления доступом);
- состояние выходов тревоги средств сигнализации и управления доступом в различных режимах, так как отечественные и большинство зарубежных средств охранной сигнализации имеют в дежурном режиме на выходе замкнутые контакты, которые размыкаются при тревоге.

6. ТИПОВЫЕ ВАРИАНТЫ СКУД

6.1. Автономные СКУД

Автономными СКУД, обычно оборудуются: квартиры, коттеджи, небольшие офисы, магазины, аптеки, гостиницы и т.п. и мало значимые зоны на важных объектах. Данные СКУД это небольшие и недорогие системы, обслуживающие, как правило, до 8-ми устройств заграждения (дверей, ворот, турникетов и т.п.).

На рисунке 1 приведен вариант контроля и управления доступом в помещение с одной дверью. На рисунке представлен полный состав системы, в который входит: контроллер, совмещенный со считывателем, кодонаборная клавиатура, исполнительное устройство (замок), датчик состояния двери, кнопка автоматического открывания двери с внутренней стороны, внешние звуковой и/или световой оповещатели, источник питания.

Система, приведенная на рисунке 1, обеспечивает два способа контроля доступа: проверку только карточек или двойную проверку - карточек и кодового пароля.

В системе можно устанавливать, так называемый, офисный режим. Его смысл состоит в том, что пользователь открывает закрытый замок с помощью идентификатора и проходит в помещение. Далее снаружи открывать замок можно свободно, простым нажатием ручки. Этот режим устанавливается по желанию пользователя, например, для того, чтобы каждый раз не подходить к двери (не нажимать кнопку автоматического открывания двери) и открывать ее изнутри, когда стучатся посетители.

При реализации данного варианта на объекте рекомендуется:

- использовать системы, имеющие прочный металлический корпус, кодонаборную клавиатуру с металлическими кнопками, встроенную индикацию режимов работы, антисаботажную защиту для предотвращения умышленного взлома корпуса контроллера и считывателя;

- использовать системы имеющие энергонезависимую память и позволяющие хранить данные длительное время;
- использовать системы позволяющие изменять время разблокировки дверей;
- программирование системы осуществлять с помощью мастер-карточки и клавиатуры.

Данный состав СКУД может варьироваться в широких пределах и в минимуме состоять из одного конструктивно законченного блока (в виде замка), в котором размещены считыватель, контроллер, исполнительное устройство (запор, ригель, задвижка и т.п.), индикаторы режимов работы. При этом СКУД работает в режиме обычного замка, т.е. при совпадении кодов идентификатора и считывателя запорный механизм срабатывает и разблокирует дверь, разрешая через нее проход.

В процессе расширения системы дополнительно может устанавливаться еще один считыватель для контроля прохода в обратную сторону (или организации многоуровнего контроля доступа), выносные световые/звуковые оповещатели, устройства автоматического открывания/закрывания двери и т.д.

На рисунке 2 приведен вариант оборудования СКУД, работающей в автономном режиме, объекта с несколькими дверями. Данный вариант построения системы отличается от предыдущего только лишь расширением функций и объемом памяти управляющего контроллера, а также его конструкцией. Считыватели и исполнительные устройства размещены в разных конструктивных блоках и управление ими осуществляется через общий контроллер.

В систему могут быть введены дополнительные функции:

- контроль прохода в двух направлениях;
- автоматическое открытие и закрытие дверей при аварийных и тревожных ситуациях;

- передача тревожных сообщений на пост охраны;
- регистрация происходящих событий с помощью принтера, подключаемого к контроллеру.

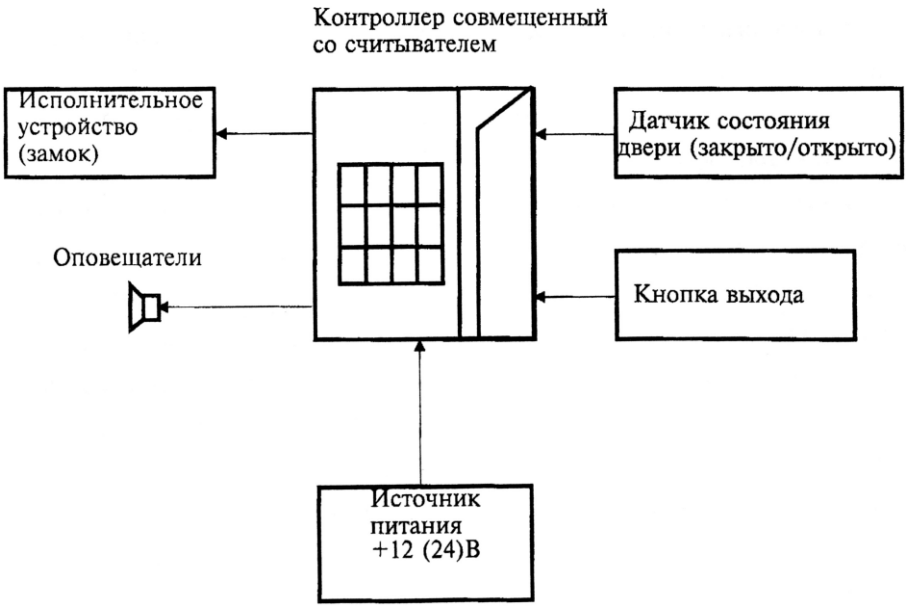


Рис. 1. Оборудование СКУД помещения с одной дверью

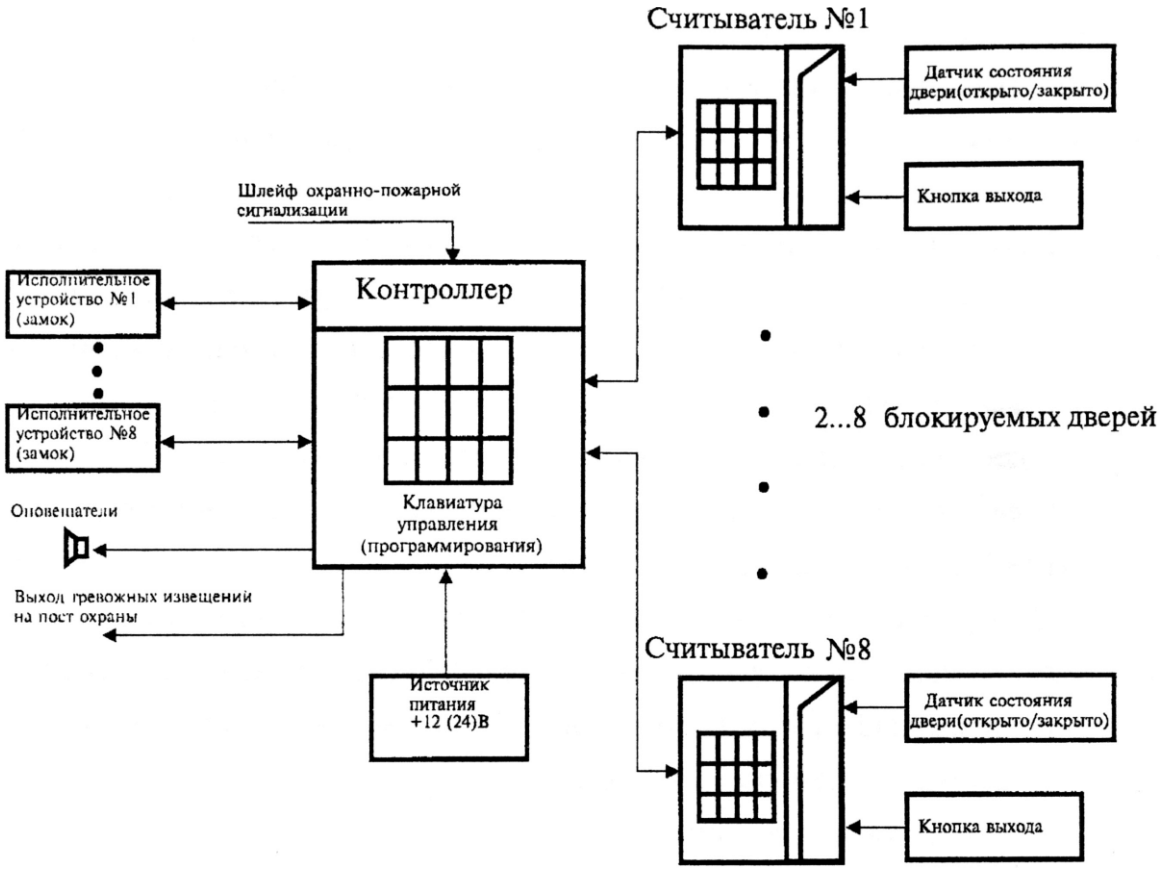


Рис. 2. Оборудование СКУД объекта с несколькими дверями

Программирование системы осуществляется как с помощью мастер-карточки и клавиатуры, так и с помощью переносного компьютера.

В своем законченном виде данную систему можно легко включить в СКУД, работающую в сетевом режиме. Для этого необходимо использовать контроллер позволяющий работать в сетевом режиме с другими контроллерами или использовать дополнительный модуль связи, обеспечивающий объединение контроллеров посредством интерфейса.

6.2. Сетевые СКУД

Сетевые СКУД предназначены для оборудования крупных объектов таких как банки, крупные учреждения и офисные здания. Несомненным достоинством этих систем является возможность практически не ограниченного расширения. Такие системы позволяют обслуживать десятки тысяч пользователей.

Эффективность работы сетевых СКУД , обусловлена возможностью создавать разветвленные, достаточно многочисленные соединения контроллеров и управляющих компьютеров в единую систему. Модульность построения данных систем обеспечивает:

- гибкость конфигурации;
- простоту монтажа, технического обслуживания и ремонта;
- возможность расширения системы;
- ценовую эффективность;
- легкость сопряжения с устройствами сервисной автоматики (управление лифтом, освещением, системами кондиционирования и т.д.).

На рисунке 3 приведена примерная структурная схема построения сетевой СКУД (64 контролируемые двери) на базе многофункционального контроллера, имеющего модульную конструкцию. На рисунках 4-6 приведены варианты построения сетевых СКУД с ветвлением.

Соединение контроллеров между собой и подключение контроллера к различным периферийным устройствам, входящим в состав системы обеспечивается при помощи различных модулей.

К одному контроллеру может быть подключено до 8 считывателей различного типа, например, считыватель магнитных карточек, считыватель бесконтактных карточек, клавиатура (кодонаборное устройство) и д.р. Подключение считывателей осуществляется через соответствующий считывающий модуль, работающий с двумя считывающими устройствами. Помимо считывателей, он также контролирует датчики состояния дверей и кнопки их открывания, другие вспомогательные устройства. Информация о состоянии иных внешних устройств поступает в контроллер через модуль входа/выхода. Посредством этого же модуля контроллер управляет работой исполнительных устройств, устройством выдачи тревожных извещений. Модуль связи обеспечивает объединение контроллеров в единую систему, протяженностью до 1 км с помощью интерфейса RS-485, а также при необходимости объединение контроллеров и управляющего компьютера в компьютеризированную систему с помощью интерфейса RS-232. Модуль приема-передачи управляет работой считывателей бесконтактных карточек (Proximity). Один контроллер может обслуживать до 10000 пользователей. Для увеличения числа пользователей может применяться модуль расширения памяти.

При создании компьютерной сети контроллеры в количестве до 32 единиц могут быть объединены в одну ветвь в соответствии с рисунком 4. В этом случае модуль связи включается в первый по порядку контроллер ветви. Через него осуществляется связь этого контроллера с компьютером по интерфейсу RS-232. Обмен информацией между контроллерами производит по интерфейсу RS-485. Кроме того, модуль связи осуществляет преобразование формата и скорости передачи данных RS-232/RS-485. Каждый контроллер в ветви имеет свой уникальный адрес.

Дальнейшее наращивание системы возможно путем организации нескольких (до 10) ветвей контроллеров. Пример организации двух ветвей показан на рисунке 5. Модуль связи первого контроллера преобразовывает с одной стороны поток данных, посылаемых с управляющего компьютера на контроллер, а с другой - поток выходных данных, параллельно подаваемых на адресные модули связи в ветвях. Каждый адресный модуль связи обменивается данными с контроллерами в ветвях и модулями связи. Такая расширенная сеть позволяет обслуживать до 320 контроллеров и 2048 контролируемых точек.

При необходимости ветвь контроллеров может быть увеличена еще на 1 км. Для этого удлиняемая ветвь (см. рисунок 6) подключается к первому контроллеру новой ветви через модуль связи. Для связи между контроллерами по-прежнему используется интерфейс RS-485.

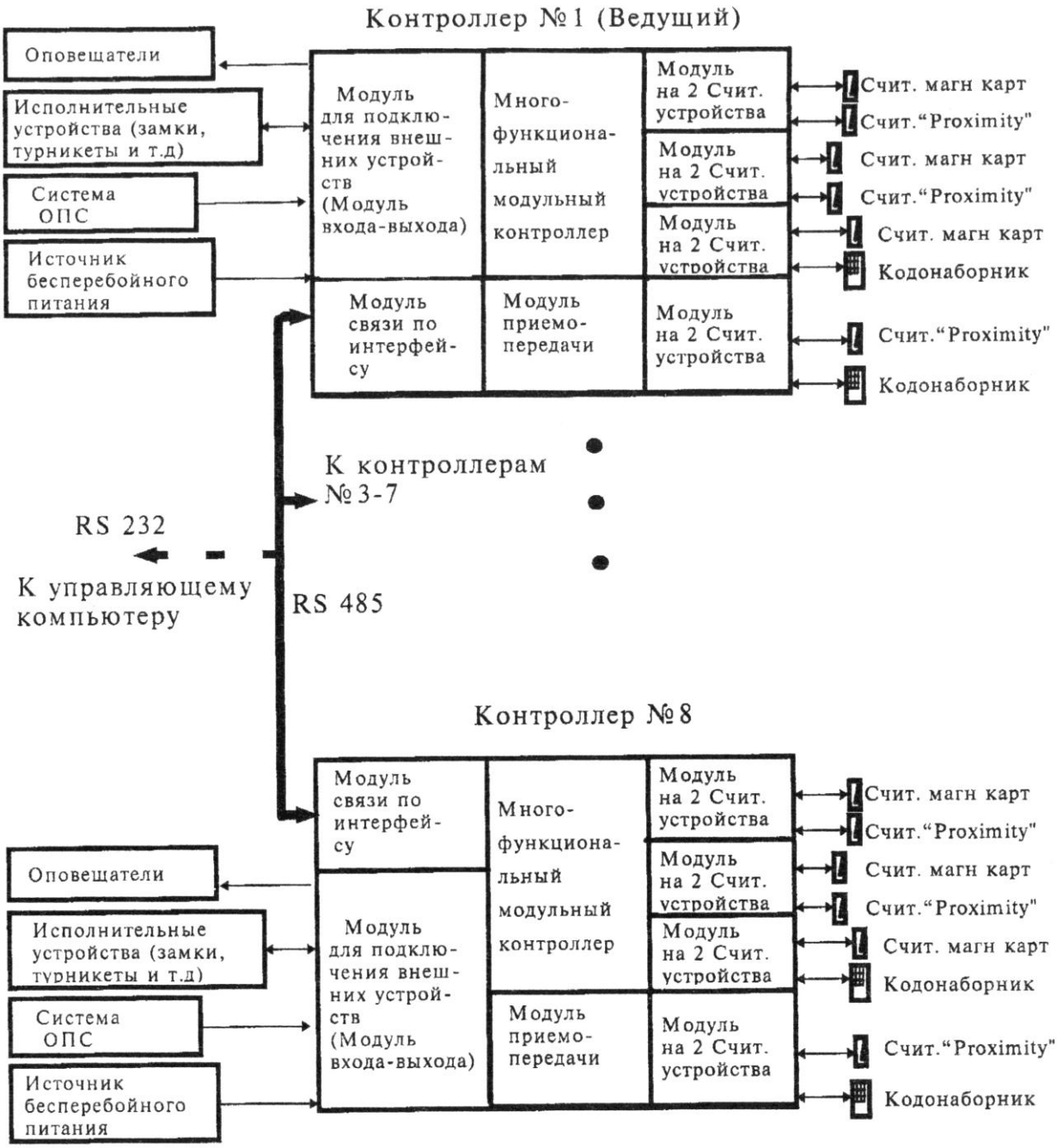


Рис. 3. Примерная структурная схема построения сетевой СКУД

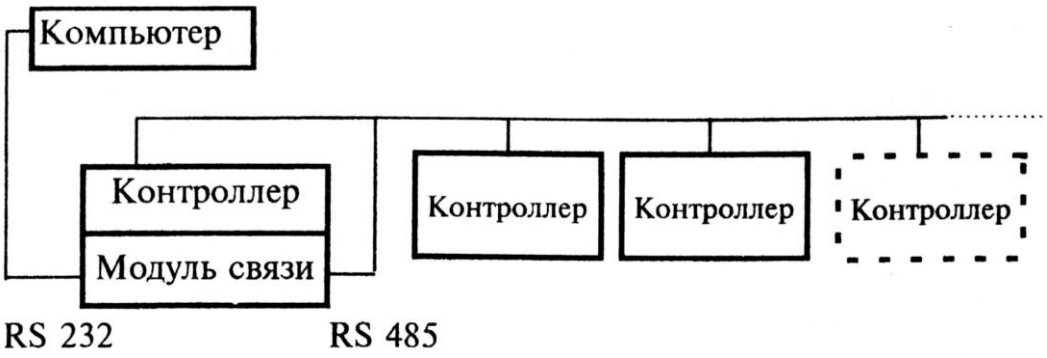


Рис. 4. Примерная структурная схема построения сетевой СКУД с одной ветвью

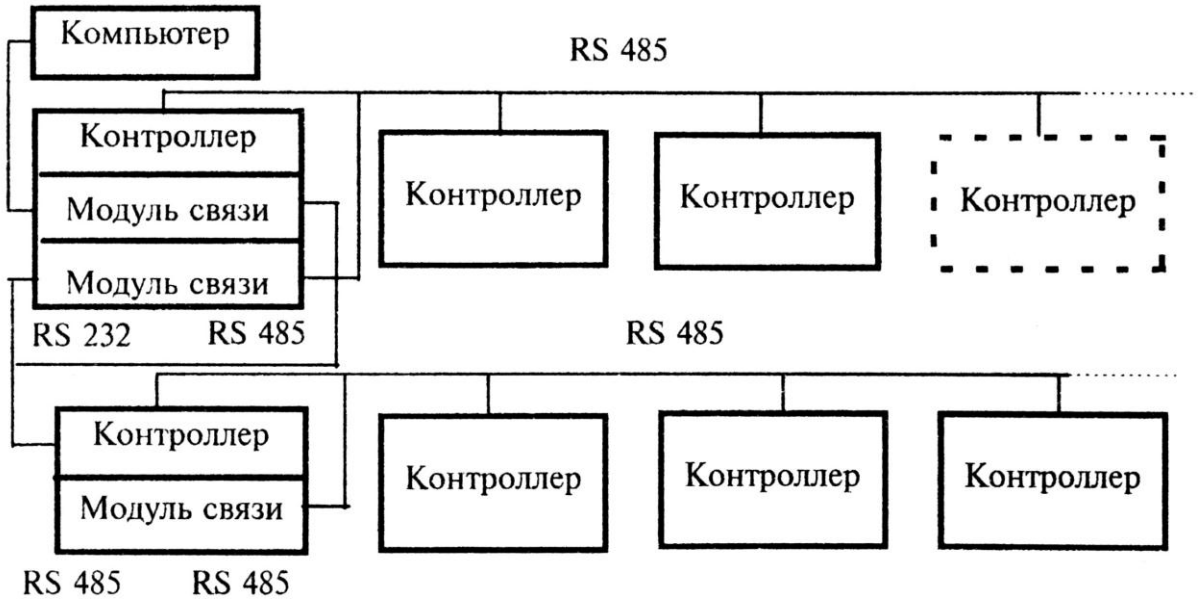


Рис. 5. Примерная структурная схема построения сетевой СКУД с несколькими ветвями

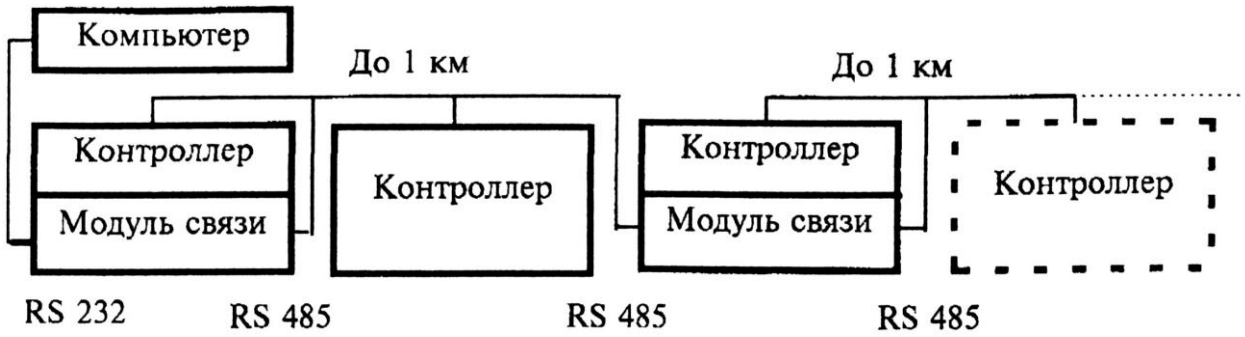


Рис. 6. Увеличение длины ветви при использовании двух модулей связи

Наличие описанных модулей многофункционального контроллера создает большие возможности по управлению разнообразной периферией системы. В качестве контролируемых точек могут выступать замкнутые/разомкнутые контакты кнопок, реле, выходные контакты различных объемных или поверхностных извещателей.

В качестве исполнительных устройств могут использоваться электрозамки дверей, исполнительные устройства шлагбаумов, турникетов, устройства тревожного оповещения и освещения, телевизионные камеры и т.д.

Логическое устройство (процессор) контроллера позволяет производить необходимую установку параметров доступа в каждой контрольной точке при помощи программного обеспечения, то есть конфигурировать систему. Системный оператор может задавать параметры (замкнутое/разомкнутое состояние контактов реле или кнопок, состояние и режим работы счетчиков, состояние флатовых регистров, временные интервалы регистраторов событий и т.д.) прямо с клавиатуры компьютера. Это дает возможность реализовывать различные варианты организации контроля и управления доступом, гибко меняя их в соответствии с текущими требованиями.

Программа предоставляет большие сервисные возможности оператору, выводя разнообразную информацию на экран. Например, на дисплее компьютера можно иметь план одного или нескольких помещений с обозначенными на нем контролируемыми точками, индикацию несанкционированных проникновении (если требуется - со звуковым сопровождением). На экран могут выводиться многочисленные сообщения, например, полные или краткие отчеты о зарегистрированных событиях с возможностью их распечатки на принтере.

7. РАЗМЕЩЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ СКУД НА ОБЪЕКТЕ

7.1. Устройства центрального управления

Устройства центрального управления (персональные компьютеры), являющиеся "мозгом" СКУД рекомендуется устанавливать в отдельных служебных помещениях, защищенных от доступа посторонних лиц, например в помещении службы безопасности или помещении поста охраны объекта.

Основные положения, в соответствии с которыми разрабатываются режимы работы всей системы безопасности, определяются руководящим составом службы безопасности, исходя из общей концепции обеспечения

безопасности объекта. Управляющие программы загружаются в центральный управляющий и вспомогательные компьютеры или контроллеры и запираются 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 (см. рисунок 7).

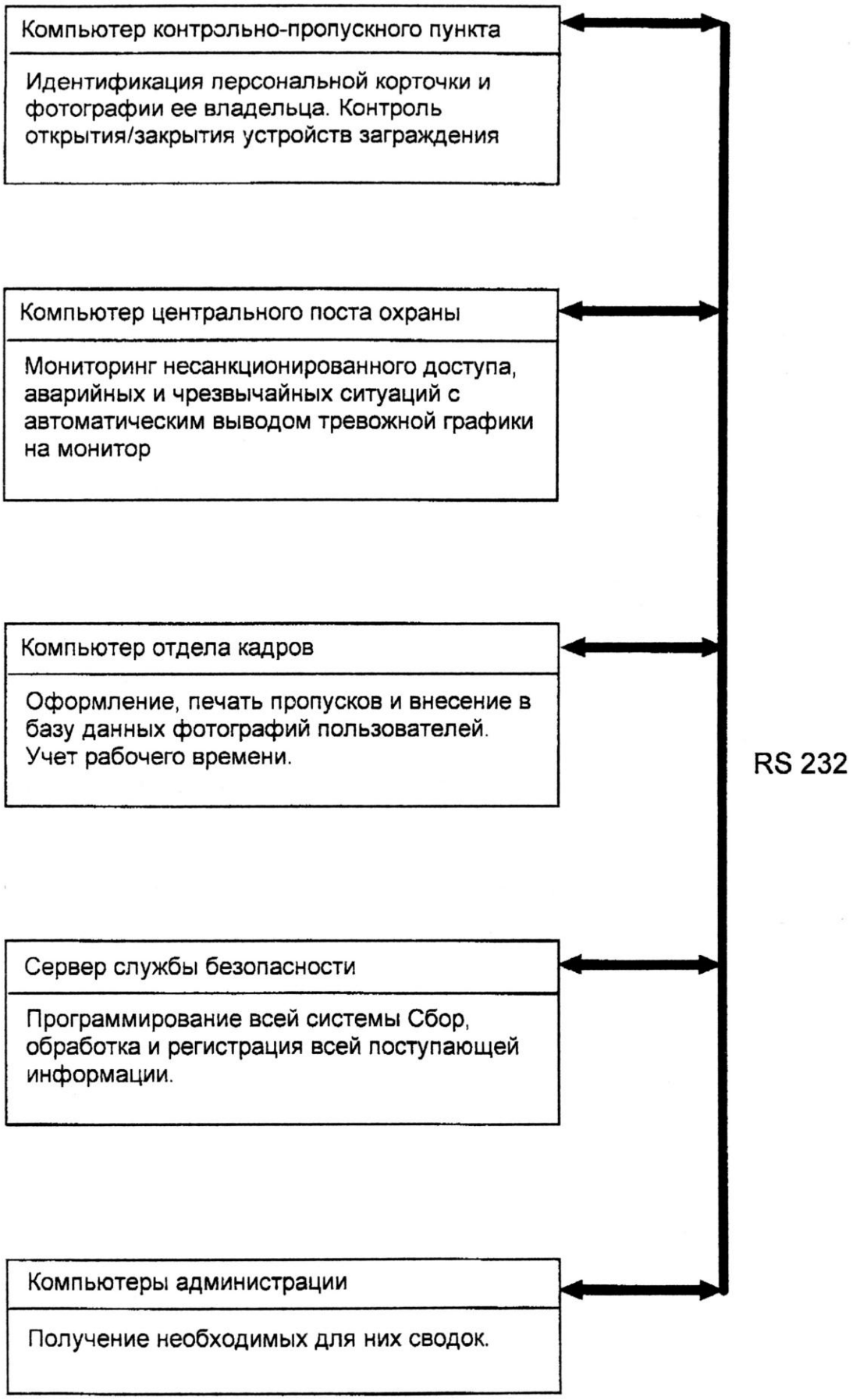


Рис. 7. Примерное размещение компьютеров СКУД, объединенных в сеть, на объекте

7.2. 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. Контроллеры, совмещенные в одном корпусе с исполнительными или считывающими устройствами рекомендуется оборудовать антисаботажными кнопками, предотвращающими несанкционированное вскрытие корпуса. Корпус данных контроллеров должен быть выполнен из ударопрочного материала, предотвращающий контроллер от актов вандализма. Контроллеры, управляющие работой считывателей или исполнительных устройств одной двери в двух направлениях, рекомендуется устанавливать с внутренней стороны охраняемого помещения.

Во избежание выхода контроллеров из строя или сбоев в работе не рекомендуется подключать их к источнику питания, от которого одновременно питается исполнительное устройство с большой индуктивностью обмоток, приводящее к броску напряжения по цепи питания. Для исключения этих нежелательных последствий необходимо предусматривать установку специальных демфирующих устройств или элементов, гасящих импульсные помехи, вызванные э.д.с. самоиндукции обмотки исполнительного устройства.

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:

- для шины RS-485 использовать высококачественный экранированный кабель витой пары;

- 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 оплетки 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.

7.3. 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, надежность и вандалостойкость. На рисунках 8 и 9 приведены некоторые варианты размещения и монтажа считывателей и устройств исполнительных.

Считыватели "Proximity" удобнее всего размещать на стене, скрытно в стене перед устройствами заграждения или даже с внутренней стороны устройства заграждения, например, на внутренней стороне неметаллической двери, если ее 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.

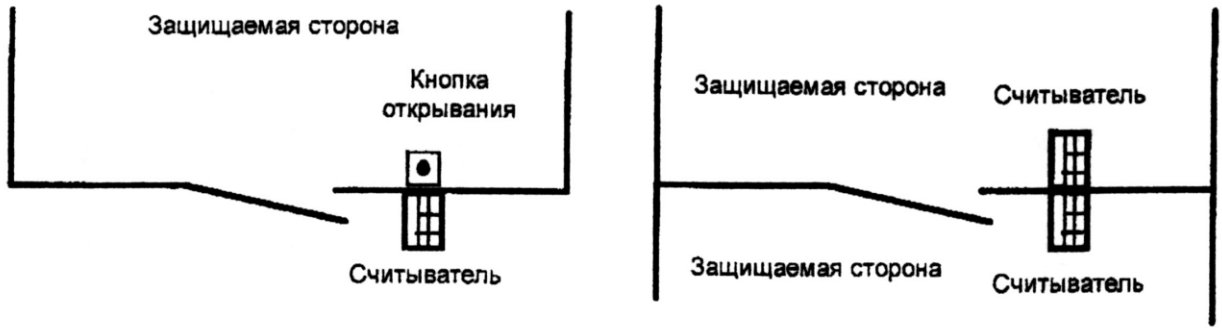
Считыватели магнитных, Виганд (Wiegand) карточек, электронных ключей и клавиатуры также рекомендуется размещать на стене или непосредственно на устройстве заграждения, на высоте удобной для пользования.

Считыватели магнитных карточек (за исключением совмещенных 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.).

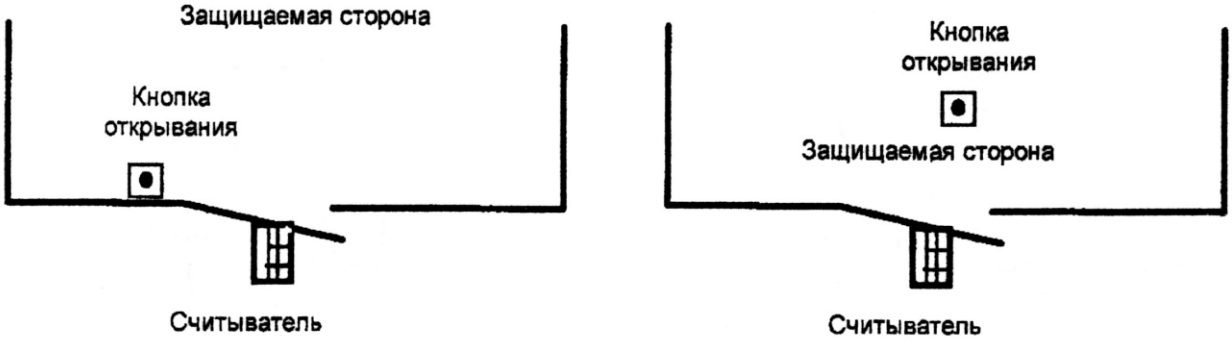
Электромагнитные защелки рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери при закрывании двери и разблокировать замок при подаче сигнала от контроллера. Кроме того такая установка защелки позволяет полностью сохранить замочно-скобяную 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 надежности и срока службы. Обычно 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, делают этот замок практически вечным. Особенность 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 надежной работы необходимо дублирование его механическим замком или применение дополнительного резервного питания.
При совместном использовании магнитноконтактных извещателей (типа СМК) в качестве датчиков положения двери с электромагнитными и электромеханическими замками, они должны быть разнесены друг от друга как можно дальше.

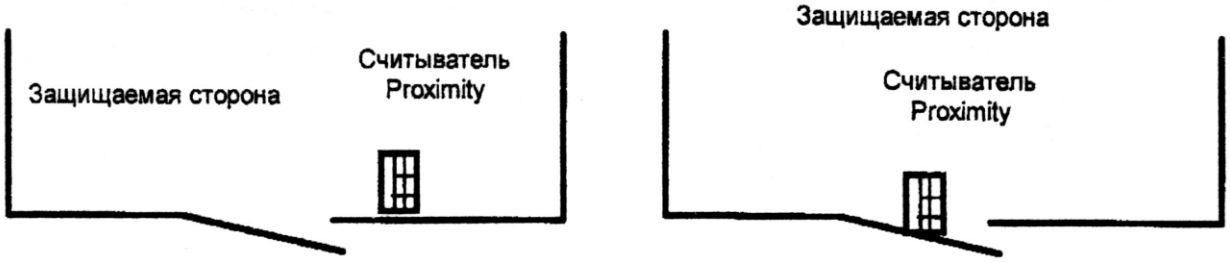
При установки исполнительных устройств (замки, доводчики, приводы и т.п.), требующих для своей работы подводки электропитания, необходимо использовать специальные устройства и кабели, обеспечивающие электро- и пожаробезопасность (особенно на сгораемых конструкциях), а также защиту от повреждений при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



Размещение считывателей на стене

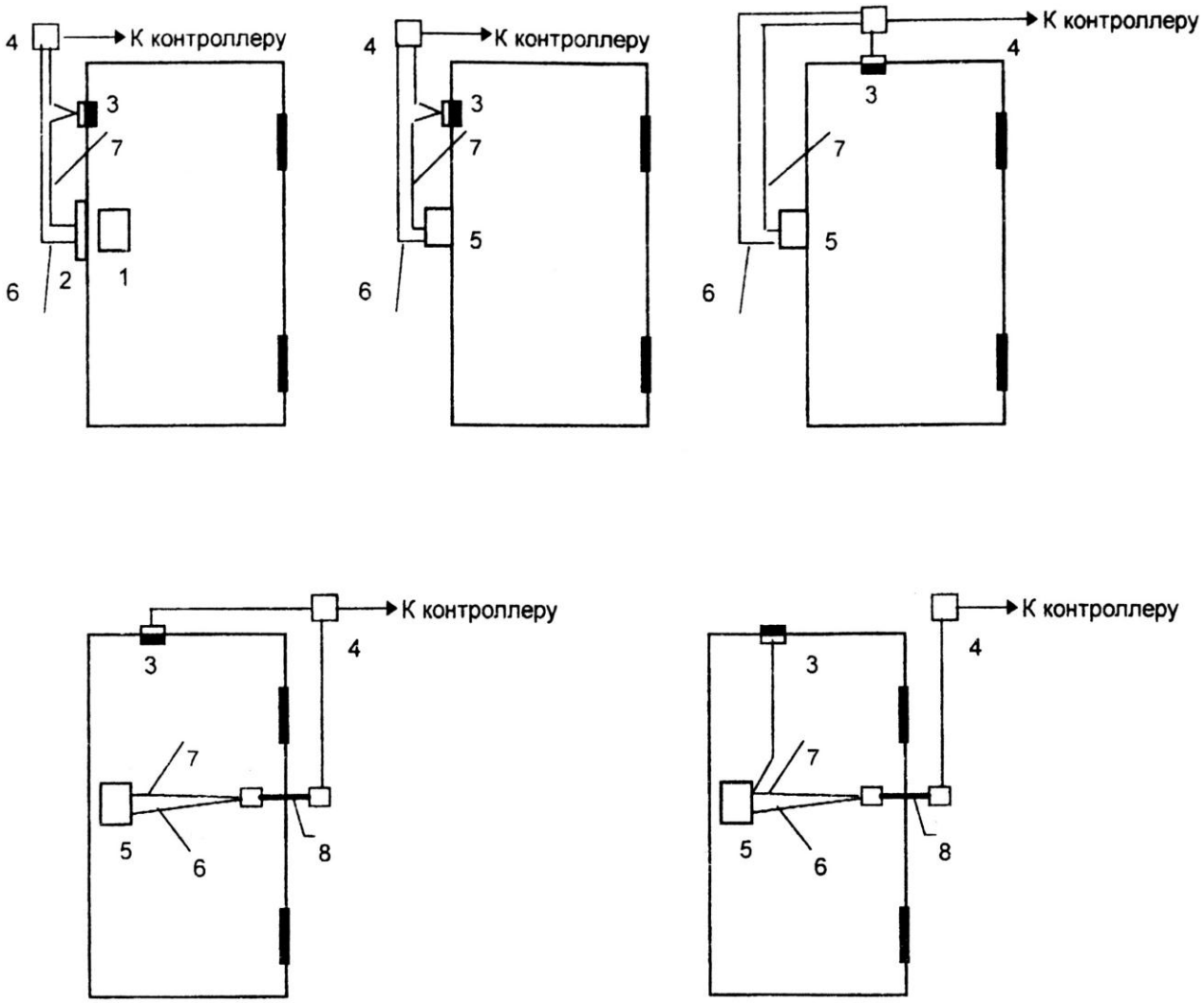


Размещение считывателей на двери



Размещение считывателей за стеной и за дверью

Рис.8. Варианты размещения считывателей



Условные обозначения:
1 - Механический замок
2 - Электромагнитная защелка
3 - Магнитоконтактный датчик открытия двери (СМК)
4 - Соединительная коробка
5 - Электромеханический или электромагнитный замок
6 - Кабель питания замка (для дверей из сгораемого материала двойная изоляция ПХВ или металлорукав)
7 - Цепи управления и контроля
8 - Гибкий переход (кабелепровод)

Рис. 9. Варианты размещения исполнительных устройств на дверных конструкциях

8. МОНТАЖ ЭЛЕКТРОПРОВОДОК ТЕХНИЧЕСКИХ СРЕДСТВ СКУД НА ОБЪЕКТЕ

8.1. Электропроводки технических средств СКУД

Электропроводки технических средств СКУД представляют собой совокупность кабельных линий и линий проводов электрических соединителей, трубопроводов и коробов, проложенных и закрепленных на элементах зданий и сооружений, для прокладки кабелей и проводов, устройств их крепления и защиты от механических повреждений. Для монтажа электропроводок рекомендуется применять кабели и провода, перечень которых приведен в таблице 2, за исключением случаев, когда кабельная и проводная продукция входит в комплект поставки или оговорена в технической документации на СКУД.

Следует помнить, что при большой длине электропроводок (более 50 м) для борьбы с электромагнитными помехами необходимо использовать экранированные кабеля и провода, витые пары. Сечение (диаметр) проводников выбирается исходя из длины электропроводки и нагрузки. Кроме того выбор видов электропроводки, проводов, кабелей, труб и коробов с проводами и кабелями и способов их прокладки должен осуществляться с учетом требований электро- и пожарной безопасности.

Электропроводки СКУД подразделяются на:

- линии связи (цепи сигнализации и управления, шины данных, интерфейсные шины), обеспечивающие связь между исполнительными устройствами, считывателями, контроллерами и компьютерами;
- низковольтные цепи питания (12/24 В постоянного тока);
- высоковольтные цепи питания (220/380 В переменного тока частотой 50 Гц).

Таблица 2. Рекомендуемый перечень проводов и кабелей

Марка кабеля	Число жил (пар)	Сечение жил, мм2 (диаметр, мм)	Способ прокладки	Область применения	Примечание
АВВГ, АПВГ ГОСТ 16442-80	2,3	2,5 - 50	Внутри помещений, в тоннелях, каналах	Силовые цепи электропитания	Допускается прокладка в земле в трубах
АВРГ, АНРГ, ВРГ ГОСТ 433-73Е	2; 3	2,5-50	Внутри помещений, в тоннелях, в каналах	Силовые цепи электропитания	
АПВ ГОСТ 6323-79Е		2,5-50	В стальных пустотных каналах строительных конструкций	Монтаж электрических цепей	
КРВГ, КНРГ, АКРНГ, КРВГ, АКПсВГ, КВВГ, КПВГ, КПсВГ, ГОСТ 1508-78Е	4; 5; 7; 10; 14; 19; 27; 37	0,75 - 2,5	Внутри помещений, в тоннелях, в каналах	Цепи управления и сигнализации	Допускается прокладка в земле в трубах
АКВВГ, АКПВГ ГОСТ 1508-78Е	4; 5; 7	2,5	Внутри помещений, в тоннелях, в каналах	Цепи управления и сигнализации	Кроме пожаро- и взрыво-опасных помещений
ТСВ ТУ 16-К71-005-87	(5; 10; 20; 30; 41; 103)	0,5	Монтаж оборудования	Цепи сигнализации	
ПРППМ ТУ 16.505.755-80		(0,8; 1,0; 1,2)	Внутри помещения по стенам зданий, в земле	Цепи управления и сигнализации	С медными жилами
ТРП ТУ16.К04.005-89	2	0,4 - 0,5	Внутри помещений и по наружным стенам зданий	Абонентская телефонная распределительная сеть	
ТПП, ТПВ ГОСТ 22498-88Е	(10; 20; 30; 50; 100)	(0,5; 0,7)	Внутри помещений, в канализации, по стенам зданий, на	Цепи сигнализации, местные телефонные сети	

			опорах		
ТППБ, ТППБГ ГОСТ 22498-88Е	(10; 20; 30; 50; 100)	(0,5; 0,7)	В земле в траншее	Цепи сигнализации	
ТРВ ТУ 16.К04.005-89	2	(0,4; 0,5)	Внутри помещений и по наружным стенам зданий	Абонентская телефонная распределительная сеть	
РК-75-2-12 ГОСТ 11326.70-79		(2)	Внутри помещений, по стенам зданий, в канализации	В телевизионных установках	Коаксиальный кабель
РК-75-2-13 ГОСТ 11326.71-79		(2)			
РК-75-4-11 ГОСТ 11326.8-79		(4)			
РК-75-4-12 ГОСТ 11326.9-79		(4)			
РК-75-4-15 ГОСТ 11326.22-79		(4)			
РК-75-4-16 ГОСТ 11326.23-79		(4)			
РК-75-7-15 ГОСТ 11326.24-79		(7)			
РК-75-7-16 ГОСТ 11326.25-79		(7)			
РК-75-9-12 ГОСТ 11326.26-79					
РК-75-9-13 ГОСТ 11326.12-79		(9)			
РПШ ТУ 16-505-670-74	2; 8; 10; 12; 14	0,5; 0,75; 1,0	В канализациях, по стенам зданий	Цели управления телевизионных установок и СКУД	

НВ	1	0,8-1,0		Монтаж оборудования	
НВМ ГОСТ 17515-72Е	1	0,8-2,5			
МГШВ ТУ-16-505.437-82	1	0,2-1,5		Внутри-приборный и межприборный монтаж	
МКШ, МКЭШ ГОСТ 10348-80	2; 3; 5; 7; 10; 14	0,35; 0,5; 0,75	Для прокладки внутри помещений открыто, в трубах	Монтаж приборов	
ПРППА ТУ 16.505-755-80	2	1,6	Внутри помещения по стенам здании, в земле открыто и в трубах	Цепи сигнализации и управления	
АППВ ГОСТ 6323-79Е	2,3	2,0-6	Негибкий монтаж электрических цепей	Цепи электропитания	
ППВ ГОСТ 6323-79Е	2,3	0,75 - 4	Негибкий монтаж электрических цепей	Цепи электропитания	
ПВ-1 ГОСТ 6323-79Е	1	0,5 - 95	В стальных трубах, пустотных каналах строительных конструкций, на лотках	Монтаж силовых и осветительных цепей	
ПВ-3 ГОСТ 6323-79	1	0,5 - 95	В стальных трубах, пустотных каналах строительных конструкций, на лотках	Гибкий монтаж цепей, гибкий монтаж при скрытой и открытой прокладке	
ШВВП ГОСТ 7399-80Е	2-3	0,5-0,75	Внутри помещений	Присоединения машин и приборов к сетям напряжением до	

				380 В	
ЛСВ ТУ 16.705.403-85	2, 4, 10	0,4 - 0,5	Внутри помещений, по стенам зданий	Монтаж цепей сигнализации и управления	
ПКСВ	2,3,4	0,5	Внутри помещений, по стенам зданий	Монтаж цепей сигнализации и управления	

АВВГ	- кабель с изоляцией и оболочкой из поливинилхлоридного пластиката, без защитного покрова с алюминиевой жилой, гибкий
АПВГ	- кабель с изоляцией из полиэтилена, оболочкой из поливинилхлоридного пластиката, без защитного покрова с алюминиевой жилой, гибкий
АВРГ	- кабель с поливинилхлоридной оболочкой с алюминиевой жилой, гибкий
АНРГ	- кабель с резиновой маслостойкой оболочкой, не распространяющей горение, с алюминиевой жилой, гибкий
ВРГ	- кабель с поливинилхлоридной оболочкой, с медной жилой, гибкий
АПВ	- провод с алюминиевой или алюминиевой, плакированной медью, жилой с поливинилхлоридной изоляцией
ПВ1	- провод с медной жилой с поливинилхлоридной изоляцией
ПВ2	- провод с медной жилой с поливинилхлоридной изоляцией повышенной гибкости
КРВ1	- кабель с изоляцией из резины, оболочкой из поливинилхлоридного пластиката, с медной жилой, гибкий
КРНГ	- кабель с изоляцией из резины, оболочкой из резины не распространяющей горение, с медной жилой, гибкий
АКРНГ	- кабель с изоляцией из резины, оболочкой из резины не распространяющей горение, с алюминиевой жилой, гибкий
КРВГ	кабель с изоляцией из резины, оболочкой из поливинилхлоридного пластиката, с медной жилой, гибкий
АКПсВГ	- кабель с изоляцией из самозатухающего полиэтилена, оболочкой из поливинилхлоридного пластиката, с алюминиевой жилой, гибкий

КВВГ	- кабель с изоляцией и оболочкой из поливинилхлоридного пластиката, с медной жилой, гибкий
КПВГ	- кабель с изоляцией из полиэтилена, оболочкой из поливинилхлоридного пластиката с медной жилой, гибкий
КПсВГ	- кабель с изоляцией из самозатухающего полиэтилена, оболочкой из поливинилхлоридного пластиката с медной жилой, гибкий
АКВВГ	- кабель с изоляцией и оболочкой из поливинилхлоридного пластиката, с алюминиевой жилой, гибкий
АКПВГ	- кабель с изоляцией из полиэтилена, оболочкой из поливинилхлоридного пластиката, с алюминиевой жилой, гибкий
ТПП	- кабель телефонный, с полиэтиленовой изоляцией в полиэтиленовой оболочке с алюминиевым экраном
ТПВ	- кабель телефонный, с полиэтиленовой изоляцией с алюминиевым экраном, в поливинилхлоридной оболочке
ТППБ	- кабель телефонный, с полиэтиленовой изоляцией в полиэтиленовой оболочке, с алюминиевым экраном, бронированный стальными лентами, с наружным защитным покровом
ТППБГ	- кабель телефонный, с полиэтиленовой изоляцией в полиэтиленовой оболочке с алюминиевым экраном, бронированный стальными лентами с противокоррозионным покрытием, гибкий
НВ	- провод монтажный с жилой из медных луженных проволок с изоляцией из поливинилхлоридного пластиката
НВМ	- провод монтажный с жилой из медных проволок с изоляцией из поливинилхлоридного пластиката
МКШ	- кабель с изоляцией и оболочкой из поливинилхлоридного пластиката
МКЭШ	- кабель с изоляцией и оболочкой из поливинилхлоридного пластиката, экранированный
АППВ	- провод с алюминиевыми или алюминиевыми, плакированными медью, жилами с поливинилхлоридной изоляцией, плоский с разделительным основанием
ППВ	- провод с медными жилами с поливинилхлоридной изоляцией, плоский с разделительным основанием

ШВВП	- шнур гибкий с параллельными жилами с поливинилхлоридной изоляцией, в поливинилхлоридной оболочке, на номинальное переменное напряжение до 380 В
РК	- кабели радиочастотные
ЛСВ	- ленточные провода с изоляцией из полиэтилена или поливинилхлоридного пластиката с медными луженными жилами
ТРП	- провода телефонные распределительные, однопарные с медными токопроводящими жилами с полиэтиленовой или поливинилхлоридной изоляцией
ПРППМ	- кабель с полиэтиленовой изоляцией в полиэтиленовой оболочке с медными жилами
ТРВ	- провод телефонный распределительный с медными жилами с поливинилхлоридной изоляцией
ТСВ	кабель с медными жилами, с изоляцией и оболочкой из поливинилхлоридного пластиката
ПРППА	- кабель с полиэтиленовой изоляцией в полиэтиленовой оболочке с алюминиевыми жилами
РПШ	- провода монтажные с волокнистой или пленочной и поливинилхлоридной изоляцией
МГШВ	- провода с резиновой изоляцией для радиоустановок
ВВГ	- кабель с изоляцией и оболочкой из поливинилхлоридного пластиката, без защитного покрова, гибкий
ПКСВ	- провод с поливинилхлоридной изоляцией, станционный кроссовый

8.2. Монтаж линий связи, низковольтных цепей питания

Монтаж электропроводок должен выполняться в соответствии с проектом (актом обследования и типовыми проектными решениями) с учетом требований ПУЭ, СНиП 3.05.06-85.

При открытой параллельной прокладке проводов или кабелей линий связи и силовых линий питания и освещения, расстояние между ними должно быть не менее 0,5 м, в противном случае должна быть обеспечена

защита от наводок. Это требование относится и к низковольтным цепям питания, если они запитывают мощные индуктивные нагрузки (электромагниты, соленоиды и т.п.) устройств заграждения. Трассы проводок необходимо выбрать наикратчайшими, с учетом расположения электроосветительных, радиотрансляционных сетей, водопроводных и газовых магистралей, а также других коммуникаций.

Прокладка проводов и кабелей по стенам внутри охраняемых зданий должна производится на расстоянии не менее 0,1 м от потолка, и как правило, на высоте не менее 2,2 м от пола. При прокладке проводов и кабелей на высоте менее 2,2 м от пола должна быть предусмотрена их защита от механических повреждений.

Электропроводки, проходящие по наружным стенам на высоте менее 2,5 м или через помещения, которые не подлежат защите, должны быть выполнены скрытым способом или в металлических трубах. При пересечении силовых и осветительных сетей, кабели и провода СКУД должны быть защищены резиновыми или полихлорвиниловыми трубками, концы которых должны выступать на 4-5 мм с каждой стороны перехода. При пересечении кабели большей емкости должны прилегать к стене, а меньшей емкости огибать их сверху. Кабели меньшей емкости допускается пропускать под кабелями большей емкости при прокладке их в штробах. Не допускается прокладка по стенам распределительных кабелей емкостью более 100 пар.

При выполнении скрытой проводки в полу и междуэтажных перекрытиях кабели должны прокладываться в каналах и трубах. Заделка кабелей в строительные конструкции наглухо не допускается. На прокладку скрытой проводки составляется акт.

При прокладке кабелей в местах поворота под углом 90°(или близких к нему) радиус изгиба должен быть не менее семи диаметров кабеля. Кабели и провода должны крепиться к строительным конструкциям при помощи скреб или скоб из тонколистовой оцинкованной стали,

полиэтиленовых эластичных скоб. Установка крепежных деталей должна производиться с помощью шурупов или клея. При прокладке нескольких проводов по одной трассе допускается располагать их вплотную друг к другу.

Для соединения и ответвления провода и шин рекомендуется применять распределительные и соединительные коробки. Расстояние от кабелей и изолированных проводов, прокладываемых открыто, непосредственно по элементам строительной конструкции помещения до мест открытого размещения (хранения) горючих материалов, должно быть не менее 0,6 м. При пересечение проводов и кабелей с трубопроводами расстояние между ними в свету должно быть не менее 50 мм, а с трубопроводами, содержащими горючие или легковоспламеняющиеся жидкости и газы не менее 100 мм. При параллельной прокладке расстояние от проводов и кабелей до трубопроводов должно быть не менее 10 мм, а до трубопроводов с горючими или легковоспламеняющимися жидкостями и газами не менее 400 мм.

8.3. Прокладка электропроводок в трубах

Применяемые для электропроводок стальные трубы должны иметь внутреннюю поверхность, исключающую повреждение изоляции проводов при их затягивании в трубу.

Стальные трубы, прокладываемые в помещениях с химически активной средой, внутри и снаружи должны иметь антикоррозийное покрытие, стойкое в условиях данной среды. В местах выхода проводов из стальных труб следует устанавливать изоляционные втулки. Для ответвления и соединений стальных трубных проводок как открытых гак и скрытых, следует применять коробки, ящики и т.п. изделия.

Расстояние между протяжными коробками (ящиками) не должно превышать:

- 50 м - при наличии одного изгиба труб;
- 40 м - при наличии двух изгибов труб;
- 20 м - при наличии трех изгибов труб.

Расстояние между точками крепления открыто проложенных стальных труб, как на горизонтальных, так и на вертикальных поверхностях не должно превышать:

- 2,5 м - для труб с условным проходом до 20 мм;
- 3 м - для труб с условным проходом до 32 мм;
- 4 м - для труб с условным проходом до 80 мм;
- 6 м - для труб с условным проходом до 100 мм.

Расстояние между точками крепления металлорукавов не должно превышать:

- 0,25 м - для металлорукавов с условным проходом до 15 мм;
- 0,35 м - для металлорукавов с условным проходом до 27 мм;
- 0,45 м - для металлорукавов с условным проходом до 42 мм;

Трубы с электропроводками должны быть закреплены на опорных конструкциях на расстоянии от ввода:

- в приборы - не далее 0,8 м;
- в соединительные и протяжные коробки не далее 0,3 м;
- в гибкие металлические рукава - 0,5 - 0,75 м.

Приваривать стальные трубы к металлоконструкциям не допускается. Прокладку проводов и кабелей в неметаллических (пластмассовых) трубах следует выполнять в помещениях при температуре воздуха не ниже минус 20°С и не выше плюс 60°С. Применяемые для защиты электропроводок от механических повреждений трубопроводы должны изготавливаться из

негорючих трудносгораемых материалов с нагревостойкостью не менее 105°С, согласно требованиям ГОСТ 8865-87.

Неметаллические трубы, прокладываемые открытым способом должны крепиться так, чтобы было возможно их свободное перемещение при линейном расширении или сжатии от изменения температуры окружающей среды. Крепление следует выполнять скобами, хомутами и накладками. Расстояние между точками крепления открыто проложенных полимерных труб не должно превышать:

- 1 м - для труб диаметром 20 мм;
- 1,1 м - для труб диаметром 25 мм;
- 1,4 м - для труб диаметром 32 мм;
- 1,6 м - для труб диаметром 40 мм;
- 1,7 м - для труб диаметром 50 мм;

Изменение направлений защитных труб осуществляется изгибом. При изгибе труб следует, как правило, применять нормализованные углы поворота - 90, 120 и 135 ° и нормализованные радиусы изгиба - 400, 800 и 1000мм.

В качестве гибких вставок в защитные трубы при наличии сложных поворотов и углов переходные труб из одной плоскости в другую и для устройства температурных компенсаторов следует применять гибкие металлические рукава.

Провода и кабели в трубах должны лежать свободно, без натяжения, суммарное сечение, рассчитанное по их наружным диаметрам, не должно превышать 20 - 30% от сечения трубы. Не допускается совмещенная прокладка силовых кабелей и линий связи в одной трубе.

8.4. Прокладка электропроводок в коробах

В помещениях короба должны устанавливаться на конструкциях по стенам, колоннам, под площадками, перекрытиями и т.п.

При наружной установке короба необходимо прокладывать по техническим и кабельным эстакадам.

Конструкция и способ установки коробов не должны допускать скопления в них влаги.

Для открытых электропроводок короба должны иметь, как правило, съемные или открывающиеся крышки.

При скрытых прокладках следует применять глухие короба.

Соединения коробов между собой следует выполнять без сварки болтовыми соединениями или специальными переходниками и разветвителями. Крепление коробов к конструкциям производят специальными скобами с расстоянием между ними не более 3 м.

При вертикальном расположении коробов крепление проводов и кабелей необходимо выполнять с расстоянием в 1м.
В коробах провода и кабели допускается прокладывать многослойно с упорядочением и произвольным (россыпью) взаимным расположением. Сумма сечений проводов и кабелей, рассчитанных по их наружным диаметрам, включая изоляцию и наружные оболочки, не должна превышать: для глухих коробов 35% сечения короба в свету; для коробов с открываемыми крышками - 40%.

8.5. Прокладка электропроводок напряжением 220 В

Для электроснабжения технических средств СКУД допускается использовать провода и кабели:

- провода марки ПВ, АПВ, ПРГ - в металлических трубах и металлорукавах;
- провода марки ППВ - открыто по несгораемым основаниям, а по сгораемым основаниям с подкладкой листового асбеста толщиной 3 мм;
- провода марки АППВ - скрыто в слое штукатурки;

- кабели марки ВРГ, ВВГ, АВГ, АВРГ - внутри помещений, в каналах, тоннелях, в агрессивной среде, при отсутствии механических воздействий.

Кроме того допускается использовать провода и кабеля входящие в комплект поставки, если это не противоречит противопожарным нормам.

При монтаже электропроводок не допускается:

- применять неизолированные электрические провода;
- использовать кабели и провода с поврежденной изоляцией;
- объединять слаботочные и сильноточные электропроводки в одной защитой трубе;
- перекручивать, завязывать провода; заклеивать участки проводов и кабелей бумагой (обоями); использовать плинтусы, оконные и дверные деревянные рамы.

Соединение, ответвление и оконцевание жил проводов и кабелей должны производиться при помощи опрессовки, сварки, пайки или сжимов (винтовых, болтовых и т.п.).

В местах соединения, ответвления и присоединения жил проводов или кабелей должен быть предусмотрен запас провода (кабеля), обеспечивающий возможность повторного соединения, ответвления или присоединения.

Соединение и ответвление проводов и кабелей, за исключением проводов, проложенных на изолирующих опорах, должны выполняться в соединительных и ответвительных коробках, внутри корпусов технических средств.

Не допускается применение винтовых соединений в местах с повышенной вибрацией или влажностью.

В местах прохождения проводов и кабелей электроснабжения технических средств СКУД через стены или перекрытия должны быть предусмотрены огнестойкие уплотнения (асбест, шлаковата, песок и т.п.)

Прокладка кабелей в сооружениях подземной канализации должна производиться в соответствии с проектом и оформляться актом.

8.6. Монтаж электропроводок на территории объекта

Электропроводки технических средств на территории объекта представляют собой комплекс, состоящий из линий кабельных и электрических проводов, соединительных и присоединительных устройств, металлических конструкций и коробов, проложенных и закрепленных на элементах зданий и сооружений, для прокладки кабелей и проводов, устройств их крепления и защиты от механических повреждений. Монтаж должен выполняться в соответствии с проектом и учетом требований главы 2.1, 2.3 ПУЭ-87, СНиП 3.05.07-85.

Для монтажа электропроводок, как правило, применяются кабели и провода, перечень которых приведен в таблице 2.

Прокладка электропроводок, в зависимости от требований на охраняемом объекте, должна выполняться:

- изолированными проводами - в трубах;
- бронированными кабелями - в земле, открыто на кабельных конструкциях.

При скрытом способе, кабели прокладываются в траншеях или устройствах подземной канализации, тоннелях, коллекторах.

После окончания монтажа электропроводок измеряется сопротивление изоляции электрических цепей как между всеми жилами кабеля (всеми жилами проводов в трубе (коробе)), так и между каждой жилой и металлической защитной оболочкой кабеля (между каждой жилой провода или кабеля в неметаллической оболочке и трубой, коробом, лотком, конструкцией).

Измерение сопротивления изоляции электропроводок (цепей измерения, управления, питания, сигнализации и т.п.) проводится мегаомметром на напряжение 1000 В. Сопротивление изоляции должно быть не менее 0,5 МОм Продолжительность приложения испытательного напряжения - 1 мин.

Трубы для проводок, укладываемые фундамент, закрепляются до бетонирования фундамента, на опорных конструкциях или в арматуре.

В местах выхода труб из фундамента в грунт должны быть предусмотрены проектом компенсирующие устройства против среза труб, при осадках грунта или фундамента.

Соединения труб, требующие уплотнения, выполняются с помощью муфт на резьбе с уплотнением фторопластовым уплотнительным материалом (лентой ФУМ) или пеньковым волокном на сурике. Для электропроводок, не требующих уплотнения соединений труб, допускаются безрезьбовые соединения раструбами, манжетами или гильзами.

Трубы, прокладываемые открытым способом, должны крепиться так, чтобы было возможно их свободное перемещение при линейном расширении или сжатии, от изменения температуры окружающей среды. Крепление выполняется скобами, хомутами или накладками.

Крепление стальных труб с электропроводками к техническим трубопроводам, а также крепление непосредственной приваркой труб к строительным или технологическим конструкциям не допускается.

Расстояние между протяжными коробками (ящиками), крепление труб, их изгиб и т.п. производится в соответствии с изложенным выше. Перед прокладкой кабельных линий непосредственно в земле, траншее в случае скальных грунтов устраивается подсыпка из разрыхленной земли или песка толщиной не менее 100 мм.

На участках, где вероятны механические повреждения, кабели защищаются плитами или кирпичом (кроме силикатного). В траншеях кабель укладывают свободно, на середине, с запасом 1 - 3 % по длине, достаточным для компенсации возможных смещений почвы и температурных деформаций.

Глубина укладки кабеля не менее 0,6 м. При пересечении кабеля другими кабельными линиями, они разделяются слоем земли, толщиной не

менее 0,5 м. При прокладке в одной траншее двух или более кабелей следует их располагать параллельно с расстоянием между ними не менее 100 мм.

Для кабельных линий, прокладываемых в земле или воде, должны применяться преимущественно бронированные кабели. Металлические оболочки этих кабелей должны иметь внешний покров для защиты от химических воздействий. Кабели с другими конструкциями внешних защитных покрытий (небронированные) должны обладать необходимой стойкостью к механическим воздействиям при прокладке во всех видах грунтов, а также при протяжке в блоках и трубах.

На прокладку кабелей в траншее составляется акт на скрытые работы. Прокладка кабелей в сооружениях подземной канализации, в тоннелях и коллекторах должна осуществляться в соответствии с проектом, требованиями СНиП 3.05.06-85, главы 2-3 ПУЭ-87".

При прокладке кабельных линий в сооружениях подземной канализации, тоннелях и коллекторах размещение в них кабелей следует производить:

- при двухстороннем расположении кабельных конструкций кабели контрольные и связи должны, по возможности, размещаться на противоположных сторонах;
- при одностороннем расположении кабельных конструкций контрольные кабели связи размещаются под силовыми кабелями, при этом их следует разделять несгораемыми перегородками, имеющими предел огнестойкости не менее 0,25 ч (алебастровые перегородки, стальной прокат).

В тоннелях, коллекторах и сооружениях подземной канализации прокладка бронированных кабелей должна вестись по сплошным несгораемым перегородкам, уложенным на указанные конструкции. Рекомендуется применять перегородки из асбестоцементных плит.