

Федеральная служба войск национальной гвардии Российской Федерации

ГЛАВНОЕ УПРАВЛЕНИЕ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ
(ГУВО Росгвардии)

ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА»
(ФКУ «НИЦ «Охрана» Росгвардии)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

**Выбор и применение технических средств и систем
контроля и управления доступом**

Р 064 – 2024

Врио начальника
ФКУ «НИЦ «Охрана» Росгвардии
полковник полиции

_____ В.Н. Демин
« ___ » _____ 2024 г.

Москва 2024

Методические рекомендации разработаны сотрудниками ФКУ «НИЦ «Охрана» Росгвардии Бариновым И.А., Серебряковым С.В., Вихиревым А.А. под руководством Шипулина А.В. с учетом замечаний и предложений сотрудников ГУВО Росгвардии.

Выбор и применение технических средств и систем контроля и управления доступом: Методические рекомендации (Р 064 – 2024). – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2024 – 87 с.

Методические рекомендации предназначены для использования в практической деятельности подразделений вневедомственной охраны войск национальной гвардии Российской Федерации, ФГУП «Охрана» Росгвардии и специалистов служб охраны (безопасности) объектов различных ведомств и организаций.

Введены взамен методических рекомендаций Р 064 – 2017.

ВВЕДЕНА

С _____ 2024 г.

© ФКУ «НИЦ «Охрана» Росгвардии, 2024

Настоящий документ не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения ГУВО Росгвардии

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ.....	5
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	6
ВВЕДЕНИЕ.....	11
1 Общие положения.....	12
1.1 Основные принципы работы СКУД.....	12
1.2 Примеры применения СКУД.....	13
1.3 Задачи, решаемые СКУД.....	14
1.4 Виды идентификации.....	15
1.4.1 Достоинства и недостатки видов идентификации.....	16
1.4.2 Условия применения биометрических признаков.....	19
1.4.3 Статические и динамические биометрические признаки.....	20
1.4.4 Ошибки биометрической идентификации.....	20
1.5 Способы хранения идентификационных признаков.....	22
2 Идентификаторы и считывающие устройства, применяемые в СКУД...	24
2.1 Кодонаборные панели.....	24
2.2 ИД и УС идентификации по вещественному коду.....	28
2.2.1 Идентификационные карты с линейным и двухмерным штриховым кодированием.....	28
2.2.2 Идентификационные карты с магнитным кодированием.....	32
2.2.3 Электронные ключи iButton (Touch-Memory).....	34
2.2.4 Бесконтактные идентификаторы RFID.....	38
2.3 Примеры биометрических технологий, применяемых в СКУД.....	45
2.3.1 Идентификация по отпечатку пальца.....	46
2.3.2 Идентификация по изображению лица.....	49
2.3.3 Идентификация по кровеносным сосудам.....	51
2.3.4 Идентификация по радужной оболочке глаза.....	53
2.4 Спуфинг и антиспуфинг.....	54
2.5 Мультибиометрия и многофакторные решения.....	56

3	Требования к СКУД физического доступа	58
3.1	Построение и варианты развертывания СКУД.....	60
3.2	Требования к средствам КУД.....	61
3.2.1	Требования к ИД и УС	62
3.2.2	Требования к СУ.....	63
3.2.3	Требования к УПУ.....	64
3.3	Требования по защите информации в СКУД.....	68
3.4	Требования надежности.....	69
3.5	Требования электромагнитной совместимости	70
3.6	Требования безопасности	70
3.7	Требования устойчивости к климатическим и механическим воздействиям	71
3.8	Требования к электропитанию	71
3.9	Требования к технической документации	72
4	Выбор СКУД для оборудования объекта	73
4.1	Принципы выбора СКУД для объекта	73
4.2	Принципы построения СКУД объекта.....	74
4.3	Обследование объекта.....	76
5	Проектирование СКУД объекта	78
6	Размещение технических средств СКУД на объекте	81
6.1	Устройства центрального управления	81
6.2	Устройства контроля и управления.....	81
6.3	Устройства считывающие и устройства преграждающие управляемые	82
7	Ввод в эксплуатацию СКУД.....	85
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	87

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящих методических рекомендациях используются следующие сокращения и обозначения:

АКБ – аккумуляторная батарея;

ИД – идентификатор;

ИК-излучение – излучение в инфракрасном диапазоне;

ИСБ – интегрированная система безопасности;

ИЭПВР – источник электропитания вторичный с резервом;

КД – контроллер доступа;

КП – конструкция преграждающая;

КУД – контроль и управление доступом;

ПЗС-матрицы – прибор с зарядовой связью;

РОГ – радужная оболочка глаза;

СВТ – средство вычислительной техники (компьютер);

СКУД – система контроля и управления доступом;

СУ – средство управления;

ТУ – технические условия;

УИ – устройство исполнительное;

УПУ – устройство преграждающее управляемое;

УС – устройство считывающее.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящих методических рекомендациях применяют следующие термины с соответствующими им определениями:

Антиколлизия – процедура достоверного считывания нескольких радиочастотных идентификаторов в зоне считывания УС.

Антиспуфинг – методы противодействия попыткам обмана биометрических считывателей путем подмены истинного биометрического признака муляжом.

Аутентификационная информация – информация, используемая при аутентификации субъекта доступа или объекта доступа.

Аутентификация – действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

Вещественный код – код, записанный на физическом носителе (идентификаторе).

Взлом – действия, направленные на несанкционированное разрушение конструкции.

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

Вскрытие – действия, направленные на несанкционированное проникновение через УПУ без их разрушения.

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

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

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

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 др. устройства).

Идентификация – действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная совместимость – способность не менее двух технических (программно-технических) средств адекватно воспринимать одинаково представленные данные и пригодность этих средств к взаимодействию для выполнения установленных требований без возникновения нежелательных взаимных воздействий по видам функций, значениям параметров и эксплуатационным характеристикам.

Интегрированная система безопасности – система безопасности объекта, объединяющая в себе целевые функциональные системы, предназначенные для защиты от угроз различной природы возникновения и характера проявления.

Контроллер доступа – аппаратное устройство в составе средств управления СКУД.

Контроль и управление доступом – комплекс мероприятий, направленных на предотвращения несанкционированного доступа.

Контрольно-пропускной режим – порядок, устанавливающий правила доступа на объект охраны (к объекту охраны).

Копирование – действия с идентификаторами, целью которых является получение копии идентификатора с действующим кодом.

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

Манипулирование – действия с устройствами контроля доступа, находящимися в рабочем режиме, без их разрушения, с целью получения действующего кода или приведения в открытое состояние УПУ. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него; следы такого действия будут незаметны. Манипулирование включает в себя также действия над программным обеспечением и действия по съему информации с каналов связи и интерфейсов устройств доступа.

Наблюдение – действия с устройствами контроля и управления доступом без прямого доступа к ним с целью получения действующего кода.

Несанкционированное преодоление УПУ – несанкционированное проникновение в зону доступа через УПУ с частичным перекрытием проема без его разрушения или повреждения.

Несанкционированные действия – действия с целью несанкционированного проникновения в зону доступа через УПУ.

Несанкционированный доступ – доступ субъектов или объектов, не имеющих права доступа.

Оператор СКУД – лицо, уполномоченное проводить работы по программированию и управлению системой.

Пользователь СКУД – субъект, в отношении которого осуществляются мероприятия по контролю доступа.

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

Преграждающая конструкция – конструктивное препятствие проникновению нарушителя в охраняемые зоны, обеспечивающее блокировку в точке доступа или создающее задержку его продвижению.

Принуждение – насильственные действия по отношению к лицу, имеющему право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.

Пропускная способность – способность средства или системы пропускать через заданную точку доступа определенное число субъектов или объектов доступа в единицу времени.

Пропускной управляемый турникет (турникет) – автономное УПУ (или составная часть СКУД) с частичным или полным перекрытием проема, предназначенное для санкционированного пропуска потока людей.

Противокриминальная защита объектов и имущества – деятельность, осуществляемая с целью обеспечения криминальной безопасности

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

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

Санкционированный доступ – доступ субъектов или объектов, имеющих права доступа.

Система контроля и управления доступом – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Спуфинг – метод обмана биометрических считывателей путем подмены истинного биометрического признака муляжом.

Средства контроля и управления доступом – механические, электромеханические устройства и конструкции, электрические,

электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом.

Средства управления – 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.

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

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.

Устройства исполнительные – 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).

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

Устройство считывающее, считыватель – устройство, предназначенное для считывания (ввода) идентификационных признаков.

ВВЕДЕНИЕ

Одним из обязательных мероприятий по обеспечению противокриминальной защищенности объектов (территорий), в том числе подлежащих обязательной охране войсками национальной гвардии Российской Федерации, является оснащение охраняемых объектов системами контроля и управления доступом.

Правильное построение и использование СКУД позволяет предотвратить несанкционированный проход (проезд) на территорию охраняемого объекта, в здание, отдельные этажи и помещения. В то же время система не создает препятствий для прохода персонала и посетителей в разрешенные для них зоны. Следует помнить, что СКУД не устраняет необходимость контроля со стороны человека, но значительно повышает эффективность работы службы охраны (безопасности), особенно при наличии многочисленных зон повышенного риска возникновения криминальных или террористических угроз. СКУД является вспомогательным средством персонала охраны (безопасности) при обеспечении идентификации людей и транспортных средств и позволяет качественно выполнять основные функции по охране объекта и защите сотрудников и посетителей от преступных посягательств.

Целью настоящих рекомендаций является оказание помощи сотрудникам (работникам) подразделений вневедомственной охраны войск национальной гвардии Российской Федерации, ФГУП «Охрана» Росгвардии и специалистам служб охраны (безопасности) объектов различных ведомств и организаций в правильном выборе и проектировании системы и отдельных компонентов КУД.

1 Общие положения

1.1 Основные принципы работы СКУД

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

Каждый из пользователей СКУД 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 или 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 особенности организма человека (биометрические данные) такие, как отпечатки пальцев, геометрия кисти руки, образ лица и т.д.).

Работа СКУД происходит следующим образом. У входа в контролируемое помещение (зону доступа) устанавливаются специальные устройства – считыватели (УС), которые предназначены для считывания информации с идентификатора (ИД), ввода пароля или кодового числа, определения биометрических данных человека. Далее информация поступает на КД, которые на основании анализа данных о владельце реагируют соответствующим образом, и обеспечивают управление

преграждающими и исполнительными устройствами: открывают или блокируют дверь, включают сигнал тревоги, регистрируют присутствие человека на рабочем месте и т.д.

1.2 Примеры применения СКУД

Первичной задачей СКУД было разграничение физического доступа пользователей СКУД и транспорта на объекте и защита материальных ценностей от повреждения или кражи.

С развитием вычислительных систем встал вопрос о логическом доступе (доступе к информационным ресурсам), как способе предотвращения утечки персональных данных и промышленного шпионажа.

В дальнейшем СКУД стали интегрировать с кадровыми и бухгалтерскими программами учета рабочего времени сотрудников и фиксации времени въезда и выезда автотранспорта.

Включение в состав СКУД автоматизированной системы учета и выдачи пропусков для посетителей позволило значительно улучшить сервисное обслуживание и сократить временные и трудовые затраты при допуске посетителей объекта.

Функция СКУД, позволяющая учитывать местонахождение сотрудников, посетителей, транспорта и материальных ценностей, как в режиме реального времени, так и получая отчеты, привязанные к местоположению и времени их нахождения, вести документирование событий на объекте, приобретает особо важное значение при возникновении и ликвидации последствий чрезвычайных ситуаций.

СКУД может применяться для контроля за несением службы персоналом охраны при патрулировании объекта.

Зафиксированные события в СКУД могут служить (использоваться) для аналитики бизнес-процессов, происходящих на объекте, например,

для построения логистических цепочек автоперевозок и перемещения грузов.

СКУД используется при организации обеспечения технологической и производственной безопасности на объекте (физический не допуск персонала во время опасных технологических процессов). Включение в состав СКУД подсистем контроля взрывоопасных, радиоактивных и иных не допустимых к проносу веществ препятствует актам терроризма. Наличие в составе СКУД на проходных объекта алкотестеров позволяет предотвратить производственный травматизм, вызванный неадекватным поведением сотрудников.

СКУД, как наиболее информационно и технологически наполненная систем, может служить основой для построения ИСБ.

1.3 Задачи, решаемые СКУД

В процессе работы любая СКУД должна решать следующие задачи (выполнять процедуры):

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

– идентификацию – процедуру опознавания пользователя по предъявленному идентификатору;

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

– аутентификацию – установление подлинности пользователя по признакам идентификация;

– разрешение или отказ в доступе – выполняется на основании

результатов анализа предыдущих процедур;

– регистрацию – 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 СВТ системы и/или память контроллера. Все остальные процедуры могут производиться системой автоматически. Очевидно, что процедура аутентификации пользователя может быть выполнена полноценно только с помощью биометрической идентификации.

1.4 Виды идентификации

В соответствии с ГОСТ Р 54412-2019 (ISO/IEC TR24741:2018) определены три вида идентификации личности:

– идентификация по запоминаемому коду (признаку), все что человек может запомнить и воспроизвести может служить запоминаемым идентификатором (например, ФИО, данные паспорта, дата рождения, условное слово, кодовая последовательность цифр, букв или знаков, последовательность движений рук, тела и так далее). Иногда этот тип идентификации называют идентификация знания (я знаю, значит имею право доступа);

– идентификация по вещественному коду (признаку), с помощью предмета, на который или в который с помощью каких-либо физических явлений занесена идентификационная информация. Иногда этот тип идентификации называют идентификацией владения (я владею предметом, значит имею право доступа);

– идентификация по биометрическому признаку или биометрия. Иногда этот тип идентификации называют идентификация обладания (я обладаю биометрическим признаком, значит имею право доступа).

1.4.1 Достоинства и недостатки видов идентификации

Идентификация по запоминаемому коду, применяемая в СКУД, предполагает запоминание кода (пароля) пользователем. Запомненный пользователем код и является идентификатором. В качестве устройств ввода кода (считывателя) в этом случае используется цифровая или алфавитно-цифровая клавиатура, а также различные кодовые переключатели, панели или другие подобные устройства (клавиатурные считыватели).

Достоинством идентификации по запоминаемому коду является то, что для нее не требуется вещественный носитель кода. Соответственно запоминаемый код невозможно потерять, он не может быть украден, отсутствуют затраты на его изготовление.

Однако, процесс идентификации, основанный на запоминании кода пользователем, имеет ряд недостатков. Так, для повышения надежности код должен иметь как можно большее количество разрядов (знаков). Например, коды доступа многих сейфовых замков высокой секретности имеют не менее 12 разрядов. Запомнить такое количество цифр или знаков большинству людей достаточно трудно. Это приводит к тому, что код записывают на бумаге, секретность кода после этого практически теряется. Уязвимым местом идентификации по запоминаемому коду является возможность (как визуально, так и при помощи специальных технических средств) «подсмотреть» код в процессе его ввода на клавиатурном считывателе. Еще одна проблема связана с пропускной способностью систем, использующих идентификацию такого типа. При большом потоке людей через проходную, ошибки, связанные с неправильным набором кода, резко снижают пропускную способность и порождают множество конфликтов со службой охраны.

Следует отметить, что клавиатурные считыватели имеют определенные достоинства. Например, разрядность кода может быть выбрана произвольно, код может устанавливаться самим пользователем, произвольно им изменяться и быть неизвестным оператору системы. Также имеется возможность ввода дополнительных кодов, например, кода «тихой» тревоги при нападении и кодов управления.

В настоящее время идентификация по запоминаемому коду применяется в простейших автономных СКУД или в качестве дополнительной наряду с другими типами идентификации.

В основе идеи идентификации по вещественному коду лежит применение в качестве идентификаторов материальных носителей кода. Существует великое множество как видов материальных носителей, так и используемых технологий записи/чтения и хранения кода.

В современных автоматизированных системах идентификации в качестве идентификаторов используются пластиковые карты, брелоки, браслеты, механические или электронные ключи и другие подобные устройства.

Несмотря на многообразие видов вещественных идентификаторов, все они обладают общими достоинствами и общими недостатками.

К достоинствам идентификации с помощью материального носителя можно отнести стабильно высокую скорость считывания кода и как следствие, повышенную пропускную способность систем, использующих данный тип идентификации. В отличие от идентификации по запоминаемому коду при идентификации по вещественному коду, пользователю не требуется запоминать код, а достаточно иметь навык использования идентификатора, что в силу неоднородности возрастных и интеллектуально-психологических качеств пользователей может оказаться важным достоинством. Так, люди, находящиеся в состоянии стресса, дети и люди пожилого возраста с большой долей вероятности могут забыть код, но навык использования идентификатора, закрепленный

на уровне условных рефлексов, забыть практически невозможно.

Главным недостатком идентификации по вещественному коду является то, что идентификатор не имеет однозначной привязки к конкретному пользователю, следовательно, любой человек, завладев идентификатором, будет признан системой, использующей идентификацию по вещественному коду, санкционированным пользователем. И наоборот, санкционированный пользователь, утративший идентификатор (потерял или случайно не захватил его с собой), не будет признан системой, использующей идентификацию по вещественному коду.

Идентификация по биометрическому признаку – идентификация, основанная на использовании индивидуальных физических признаков или особенностей человека. Суть идентификации по биометрическому признаку заключается в том, что каждый человек обладает индивидуальными неповторимыми свойствами. Например, папиллярный рисунок пальцев и ладони, радужная оболочка глаза, геометрия лица и прочее. Эти параметры могут являться надежным идентификационным признаком, который нельзя потерять, подделать или передать другому лицу.

Запоминаемый и вещественный код относятся к так называемому присвоенному типу кода. При этом идентифицируется не сам человек (пользователь), а код, который ему присвоен. В этом состоит основной недостаток подобного вида идентификации. Код и пароль могут стать известными постороннему лицу случайно или преднамеренно. Идентификатор с вещественным кодом может быть потерян, украден или передан другому человеку по стовору. Если система работает в автоматическом режиме, то от подобных угроз она не защищена. Частично эта проблема решается применением многорубежной идентификации, например, по карточке и по запоминаемому коду. Однако это только несколько усложняет задачу для нарушителя. В этом случае ему нужно, например, украсть карточку и узнать код, что конечно сложнее, но принципиально метод многорубежной идентификации не решает задачу

защиты от подобных угроз.

Кардинальным решением этой задачи является биометрическая идентификация, которая более эффективна, так как опознание производится не по присвоенным человеку идентификационным признакам, а по физиологическим свойствам или особенностям самого человека.

1.4.2 Условия применения биометрических признаков

Универсальность – каждый человек должен обладать подобной характеристикой.

Уникальность – нет двух людей, обладающих одинаковыми биометрическими характеристиками.

Постоянство – неизменность признака во времени.

Производительность – вычислительная сложность технологии распознавания должна позволять производить идентификацию за приемлемое время.

Имитостойкость – противодействие спуфингу.

Приемлемость – пользователи СКУД и общество в целом не должно возражать против сбора данного биометрического параметра.

К сожалению, ни одна биометрическая характеристика не обладает всеми вышеперечисленными свойствами, и на практике приходится идти на компромисс по каждому пункту:

- некоторые физические ограничения препятствуют предъявлению, не все люди имеют все биометрические характеристики (инвалидность);

- существуют большие сходства между разными индивидами (близнецы);

- биометрические характеристики меняются с течением времени (старение);

- в СКУД для прохода пользователей по сложившейся практике время прохода (время идентификации плюс время разблокировки

преграждающего устройства) не должно превышать трех секунд;

- сложность и дополнительная стоимость антиспуфинговых решений;
- «приемлемость» зависит от сознания субъекта доступа (проблемы с лицевой биометрией в мусульманских странах).

1.4.3 Статические и динамические биометрические признаки

При биометрической идентификации различают статические (физиологические) и динамические (поведенческие) признаки.

Физиологические биометрические параметры, такие как отпечатки пальцев, геометрия кисти руки, изображение роговицы глаза или лица являются физическими характеристиками, которые измеряются в определенный момент времени.

Поведенческие биометрические параметры, например, подпись, походка или голос, представляют собой последовательность действий и делятся в течении определенного периода времени.

В СКУД физического доступа практически всегда применяются только статические признаки. В системах логического доступа (доступа к информации) могут применяться как статические, так и динамические признаки (доступ по клавиатурному почерку или голосовая идентификация).

1.4.4 Ошибки биометрической идентификации

При идентификации, использующей запоминаемые или вещественные коды, решение о допуске принимается при 100% совпадении вводимого кода.

Основное отличие биометрической идентификации от идентификации по запоминаемому или вещественному коду состоит в том, что она носит вероятностный характер.

Ошибки здесь возможны только при аппаратных неисправностях или программных сбоях. В биометрических системах решения принимаются на основе оценки вероятностного характера. В этом случае ошибки принятия решения о допуске неизбежны и можно говорить только о снижении вероятности появления ошибок. Уровень этих ошибок будет являться критерием качества системы и, в общем случае, должен быть указан в эксплуатационной документации. Этот критерий определяется двумя техническими характеристиками: вероятностью несанкционированного допуска и вероятностью ложного задержания.

Вероятность несанкционированного допуска – выраженное в процентах число допусков системой неавторизованных лиц.

Вероятность ложного задержания – выраженное в процентах число отказов в допуске системой авторизованных лиц.

Эти две характеристики можно изменять, уменьшая или увеличивая чувствительность анализирующих сенсоров биометрических признаков. Однако уменьшая одну величину, одновременно увеличивается другая. В данной ситуации необходимо находить оптимальное значение, определяемое поставленной перед биометрической системой задачей.

Наряду с двумя перечисленными характеристиками существует вероятность не опознания биометрического признака (в следствии некорректного предъявления, особенностей строения папиллярных узоров пальцев или ладони, маскирующих факторов лица, воздействия внешних факторов при считывании биометрического признака и т. д.).

Таким образом, можно говорить об ошибках биометрии трех родов:

– ошибка I рода – «не узнать своего», т.е. принимается решение «чужой», при этом субъект присутствует в списке зарегистрированных пользователей (для вероятности ложного отказа используется термин FRR – от английского False Rejection Rate;

– ошибка II рода – «пропустить чужого», т.е. принимается решение «свой», при этом субъект отсутствует в списке зарегистрированных

пользователей (для вероятности ложного доступа используется термин FAR – от английского False Acceptance Rate.

– ошибка III рода – принимается решение «чужой», но не по результату сравнения, а по причине невозможности достоверного считывания выбранного биометрического признака.

Величина ошибки I рода определяет защищенность системы от несанкционированного допуска и снижение ее величины более важно, чем снижение ошибки II рода. Пределы в которых находится эта величина в настоящее время составляют от 0.0001 до 0.1 процента. Ошибка II рода в основном влияет на пропускную способность системы. Если система не пропустила с первого раза, то можно ввести данные вторично. Это приводит к снижению пропускной способности, но надежность системы не ухудшается. Пределы, в которых находится эта величина в современных системах составляют от 0.1 до 1 процента.

Величина ошибки III рода зависит от типа и конструкции считывающего устройства и условий эксплуатации (обучение пользователей, температура окружающей среды, освещенность и т.д.).

1.5 Способы хранения идентификационных признаков

Централизованный – создается единая база данных всех пользователей системы, содержащая персональные данные и набор присущих (присвоенных) идентификационных признаков, а также присвоенные уровни доступа. Такой метод требует создания информационного сервера (группы рассредоточенных серверов), и организации защищенных каналов связи для обмена данными с локальными серверами, установленными на объектах. Обновление баз данных локальных серверов производится автоматически по инициативе центрального сервера. При необходимости, возникшей на объекте, внесение изменений в базу данных локального сервера производится по заявке

формируемой уполномоченными сотрудниками объекта.

Локальный – на каждом из объектов создается база данных пользователей, допуск которых санкционирован на данном объекте, содержащая персональные данные и набор присущих (присвоенных) идентификационных признаков, а также присвоенные уровни доступа. Информационный обмен данными с какими-либо сторонними серверами при таком методе не осуществляется, все полномочия по внесению изменений в базу данных сосредоточены у уполномоченных сотрудников объекта.

Децентрализованный – в смарт-карты пользователей с наивысшим уровнем доступа заносится информационное поле, определяющее уровень доступа для всех объектов. В соответствии с присвоенным уровнем доступа указанные пользователи получают право доступа, несмотря на отсутствие их идентификационных данных в локальных базах объектов. Запись, редактирование и хранение персональных данных и набора присущих (присвоенных) идентификационных признаков указанных пользователей производится аналогично централизованному методу.

2 Идентификаторы и считывающие устройства, применяемые в СКУД

2.1 Кодонаборные панели

Идентификация по запоминаемому коду осуществляется посредством ввода заведомо известного только пользователю кода (последовательность цифр или иных символов) на клавиатуре кодонаборной панели. Для ввода цифровой последовательности кода обычно используются кодонаборные панели с клавиатурой, содержащей десять цифровых клавиш и несколько служебных. Количество и расположение клавиш на панели варьируется в зависимости от их назначения и иных требований к исполнению (информативность, эстетические требования, и другие).

Ввод цифровой последовательности кода осуществляется посредством физического нажатия на клавиши или прикосновения к областям наборного поля. Клавиатуры различаются методом регистрации факта ввода необходимой цифры (символа). Наибольшее распространение получили механические, сенсорные и клавиатуры на оптопарах.

Для повышения вандалоустойчивости кодонаборных панелей используются методы регистрации ввода цифровой последовательности (касания кодонаборного поля), исключающие наличие в конструкции панели подвижных или механически уязвимых элементов. Наиболее распространенной является конструкция кодонаборного поля на оптопарах, использующих световые лучи инфракрасного диапазона (рисунок 2.1), как более устойчивого к оптическим помехам, вызванным загрязнением.

Символы кодонаборного поля нанесены заднюю стенку кодонаборной панели, не содержащую каких-либо электронных элементов или цепей. По периметру кодонаборной панели установлены свето- и фотодиоды, образующие оптопары. Каждая пара свето- и фотодиода устанавливается соответственно каждой строке и каждому столбцу кодонаборной панели

так, что перед каждым символом образуется пересечение двух взаимно перпендикулярных световых лучей.



Рисунок 2.1 – Конструкция кодонаборного поля на оптопарах

При работе кодонаборной панели светодиоды излучают узконаправленные световые лучи, которые, при отсутствии касания областей символов, попадают на фотодиоды формируя сигналы, обрабатываемые электрической схемой. При касании области символа пальцем или иным предметом происходит перекрытие двух лучей, пересекающихся над этой областью, вследствие чего они не попадают на соответствующие фотодиоды. Прерывание сигналов с двух фотодиодов позволяет электронной схеме произвести однозначную регистрацию факта касания области одного определенного символа и сформировать соответствующий сигнал во внешние цепи.

Наличие жестко закрепленных за определенными цифрами (символами) областей благоприятно сказывается на возможности определения цифр (символов), наиболее часто используемых в кодовых комбинациях, или их непосредственного наблюдения с целью

последующего несанкционированного использования. Данное обстоятельство наиболее актуально для механических клавиатур, где наиболее часто используемым цифрам (символам) соответствуют клавиши с более выраженным механическим износом, загрязнением или наоборот его отсутствием по сравнению с остальными клавишами. Данное обстоятельство снижает имитостойкость метода идентификации по запоминаемому коду и позволяет подбор кодовой последовательности, ограниченной цифрами (символами) соответствующими наиболее часто используемым клавишам.

С целью исключения указанных факторов в устройстве идентификации по запоминаемому коду может быть введена визуальная обратная связь. Наличие в кодонаборном устройстве обратной визуальной связи позволяет пользователю при вводе кода обойтись всего одной клавишей. Изображение кодонаборной панели с обратной визуальной связью приведено на рисунке 2.2.



Рисунок 2.2 – Кодонаборная панель с обратной визуальной связью

При проведении процедуры идентификации устройство ввода кодовой последовательности псевдослучайным образом генерирует

и по очереди выводит на дисплей цифры (символы). Для ввода кодовой последовательности необходимо производить нажатие клавиши в период индикации символа, соответствующего очередному символу требуемой кодовой последовательности.

Данный метод ввода кодовой последовательности исключает возможность определения кодовой последовательности по степени механического износа клавиш и затрудняет визуальное наблюдение вводимой кодовой последовательности.

К достоинствам метода идентификации при помощи использования кодонаборных панелей можно отнести:

- низкую стоимость модулей клавиатур, обладающих ограниченными функциональными возможностями и предназначенными исключительно для приема вводимой кодовой последовательности;

- возможность санкционированной дистанционной передачи кодовой последовательности (дистанционный допуск пользователей);

- отсутствие затрат на изготовление, хранение и копирование идентификатора;

- отсутствие аналого-цифрового преобразования, способствующего возникновению ошибок при проведении процедуры идентификации (для кодонаборных панелей, обладающих ограниченными функциональными возможностями и предназначенными исключительно для приема вводимой кодовой последовательности).

К недостаткам метода идентификации при помощи использования кодонаборных панелей можно отнести:

- необходимость запоминания кодовой последовательности;

- возможность подбора или визуального наблюдения вводимой кодовой последовательности (за исключением идентификатора, использующего визуальную обратную связь);

- низкий рабочий ресурс (для клавиатур на механических переключателях и резистивных сенсорах);

– подверженность кодонаборных панелей, предназначенных для размещения на открытом воздухе, к внешним механическим и климатическим воздействиям.

2.2 ИД и УС идентификации по вещественному коду

В основе идеи идентификации по вещественному коду лежит применение в качестве идентификаторов материальных носителей кода. Существует великое множество, как видов материальных носителей, так и используемых технологий записи/чтения и хранения кода. В современных СКУД в качестве материальных носителей вещественного кода используются пластиковые карты, брелоки, браслеты, механические или электронные ключи, и другие подобные предметы.

2.2.1 Идентификационные карты с линейным и двухмерным штриховым кодированием

Линейный штриховой код представляет собой нанесенный на поверхность идентификационной карты рисунок, содержащий последовательность параллельных линий, отличающихся цветом и шириной. Количество, ширина и взаимное расположение полосок определяют код идентификационной карты. Пример изображения элементов линейного штрихового кодирования приведен на рисунке 2.3.



Рисунок 2.3 – Линейный штриховой код

Пример изображения идентификационной карты с линейным штриховым кодированием приведен на рисунке 2.4.

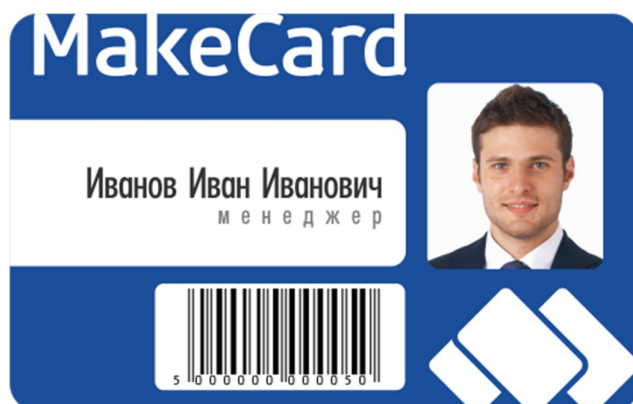


Рисунок 2.4 – Идентификационная карта с линейным штриховым кодированием

В настоящее время разработано множество типов линейного штрихового кодирования, наиболее распространенными из которых являются: EAN (EAN-8 состоит из 8 цифр, EAN-13 состоит из 13 цифр), UPC (UPC-A, UPC-E), Code56, Code128 (UPC/EAN-128), Codabar, "Interleaved 2 of 5". Двухмерные штриховые коды были разработаны для кодирования большого объема информации. Расшифровка такого кода проводится в двух измерениях (по горизонтали и по вертикали).

Двухмерные штриховые коды подразделяются на многоуровневые – stacked (см. рисунок 2.5) и матричные – matrix (см. рисунок 2.6).

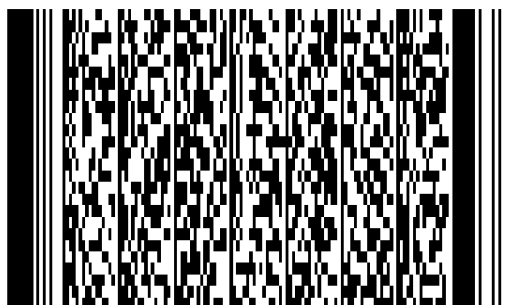


Рисунок 2.5 – Многоуровневый штриховой код



Рисунок 2.6 – Матричный штриховой код

Многоуровневые штриховые коды появились исторически ранее и представляют собой поставленные друг на друга несколько обычных линейных штриховых кодов. Матричные коды более плотно упаковывают информационные элементы по вертикали.

В настоящее время разработано множество двумерных штриховых кодов, наиболее распространенными из которых являются: Aztec Code, Data Matrix, MaxiCode, PDF417, QR код, Microsoft Tag.

Для чтения кода идентификационных карт со штрихкодом применяются считыватели, использующие оптический метод считывания.

Большинство типов считывателей способно считывать код идентификационной карты дистанционно (при поднесении ее к оптическому устройству), вместе с тем, при использовании некоторых типов считывателей, перед чтением индивидуального кода идентификационной карты требуется осуществить ее позиционирование.

Для повышения защищенности от несанкционированного копирования идентификационных карт со штриховым кодированием используются специальные непрозрачные покрытия. Чтение кода в этом случае производится в инфракрасном оптическом диапазоне. Из всех идентификационных карт со штриховым кодированием наибольшей степенью защиты обладают карты со скрытым штриховым кодом. Невидимый для глаз штриховой код впечатывается в основу карты и считывается с помощью излучения в инфракрасном оптическом

диапазоне. Индивидуальный код образуется за счет конфигурации теней при прохождении инфракрасного излучения через карту.

К достоинствам идентификаторов, использующих линейное и двухмерное штриховое кодирование, можно отнести:

- простоту изготовления идентификационной карты;
- сравнительно высокую устойчивость к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);
- большой объем кодируемой информации (для карт с двухмерным кодированием) позволяет обеспечить значительное число возможных комбинаций кодов.

К недостаткам типа идентификаторов, использующего линейное и двухмерное штриховое кодирование, можно отнести:

- легкость повторения идентификационного признака при имитации идентификационной карты;
- поверхность идентификационной карты подвержена загрязнению и истиранию, что может сказаться на правильности считывания ее кода;
- механический контакт идентификационной карты со считывателем (при позиционировании) приводит к разрушению (истиранию) как самой идентификационной карты, так и считывателя, тем самым, ограничивая срок их службы.

«Второе дыхание» идентификация со штриховым кодированием получила после массового распространения смартфонов. На сегодня это единственный тип вещественной идентификации, позволяющий передавать право доступа дистанционно. Как способ защиты от копирования дистанционно переданного кода применяют запатентованный метод динамического штрих кода. Для прохода каждый раз в приложении, установленном на смартфоне пользователя генерируется динамический штрих код. Благодаря наличию в коде точного времени генерации

при проходе пользователя считывается не только уникальный идентификатор, но и проверяется время действия, выданного штрих кода.

Полученный пользователем код действует в течение нескольких секунд, после чего обновляется и не дает возможности пройти. Поэтому нет смысла делать скриншот и пытаться делиться полученным кодом с третьими лицами.

2.2.2 Идентификационные карты с магнитным кодированием

Идентификационные карты с магнитным кодированием (магнитной полосой) достаточно широко используются в СКУД установленных в гостиницах, пансионатах, санаториях и т.д. (местах временного пребывания людей) или в качестве гостевых пропусков для посетителей. Преимуществом карт с магнитным кодированием является возможность изменения прав доступа без замены материального носителя.

Идентификационная карта с магнитной полосой состоит из пластикового основания прямоугольной формы на поверхность которого нанесена чувствительная к магнитному полю полоса (магнитная полоса) способная хранить записанную информацию на протяжении продолжительного времени. Помимо магнитной полосы в качестве вспомогательной информации на идентификационной карте могут быть нанесены текст, последовательность цифр, знаки, фотографии и т.п. Пример изображения идентификационной карты с магнитной полосой приведен на рисунке 2.7.

Для чтения (записи) кода идентификационной карты с магнитной полосой применяются считыватели, использующие магнитно-контактный метод считывания. Чтение индивидуального кода производится при протягивании магнитной полосы идентификационной карты по магнитной головке считывателя.



Рисунок 2.7 – Идентификационная карта с магнитной полосой

К достоинствам метода идентификации при помощи использования идентификационных карт с магнитным кодированием можно отнести:

- сравнительную дешевизну изготовления идентификаторов;
- возможность многократной перезаписи индивидуального кода, простота процесса перезаписи кода позволяет в случае необходимости оперативно его поменять;

- совместимость алгоритмов кодирования идентификационных карт с магнитной полосой делает возможным использование уже имеющихся у пользователя карт (например, банковских) для применения их в СКУД;

- большой объем кодируемой информации позволяет обеспечить значительное число возможных комбинаций кодов.

К недостаткам метода идентификации при помощи использования идентификационных карт с магнитным кодированием можно отнести:

- магнитно-контактный метод считывания приводит к износу как идентификационной карты, так и магнитной головки считывателя, тем самым ограничивая срок их службы (составляющий от 12 до 18 месяцев при интенсивном использовании);

– низкую устойчивость идентификационных карт к воздействию внешнего магнитного поля, что может привести к повреждению (уничтожению) кода;

– низкую устойчивость идентификационных карт к несанкционированному копированию (при наличии у злоумышленников необходимых знаний и относительно несложного оборудования);

– магнитная головка считывателя подвержена загрязнению, что может привести к неправильному чтению индивидуального кода идентификационной карты, и требует постоянного квалифицированного обслуживания;

– пользователь должен иметь навык, необходимый для правильного обращения с идентификационной картой и считывателем.

2.2.3 Электронные ключи iButton (Touch-Memory)

Электронный ключ iButton – это микросхема, заключенная в круглый герметичный корпус диаметром 16,3 мм, выполненный из нержавеющей стали. Прочный корпус обладает повышенной устойчивостью к воздействию различных внешних неблагоприятных факторов. Корпус имеет два исполнения, отличающихся по толщине: 3,1 мм (версия F3) и 5,89 мм (версия F5). Внешний вид ключей iButton представлен на рисунке 2.8, а внешний вид считывателя для ключей iButton – на рисунке 2.9.



Рисунок 2.8 – Ключи iButton

Корпус ключа iButton состоит из двух электрически изолированных друг от друга частей, являющихся контактами, через которые микросхема соединяется со считывателем. Таким образом, получается недорогой (в смысле использования аппаратных ресурсов считывающей аппаратуры) и надежный интерфейс – один провод данных и один общий провод. Энергия, необходимая для обмена информацией и работы микросхемы в корпусе, берется от провода данных.



Рисунок 2.9 — Считыватель для ключей iButton

Электронные ключи iButton имеют множество вариантов исполнений. В таблице 2.1 представлен обзор разновидностей ключей iButton.

Таблица 2.1 – Разновидности ключей iButton

Тип устройства	Family Code	Серийный номер	Количество бит, тип памяти
DS1990A	01H	есть	–
DS1991	02H	есть	512, NVRAM
DS1992	08H	есть	1К, NVRAM
DS1993	06H	есть	4К, NVRAM
DS1994	04H	есть	4К, NVRAM
DS1995	0AH	есть	16К, NVRAM
DS1996	0CH	есть	64К, NVRAM
DS1982	09H	есть	1К, EEPROM
DS1985	0BH	есть	16К, EEPROM
DS1986	0FH	есть	64К, EEPROM

Примечания:

1. Family code – код типа устройства.
2. NVRAM (NonVolatile Random Access Memory) – память с произвольным доступом на чтение и запись, с энергонезависимым хранением информации.
3. EEPROM (Electrically Erasable, Programmable Read Only Memory) – электрически стираемая память с произвольным доступом на чтение.

К достоинствам метода идентификации с использованием электронных ключей iButton можно отнести:

- сравнительно низкую стоимость самого электронного ключа, его считывателя;
- высокую степень устойчивости к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);

- корпус ключа, выполненный из нержавеющей стали, обладает повышенной устойчивостью к воздействию коррозии и агрессивных сред;

- высокие имитостойкость и степень защищенности от несанкционированного копирования (за исключением электронного ключа DS1990A), обеспечиваемые наличием кодированных областей памяти ключа;

- большой объем памяти данных, записываемых в электронный ключ, позволяет использовать многозарядные индивидуальные коды, что значительно увеличивает число комбинаций кодов;

- большой объем памяти данных позволяет записывать в электронный ключ не только его код, но и разнообразную дополнительную информацию о пользователе – носителе идентификатора;

- продолжительный срок службы ключа;

- отсутствие в электронном ключе источника электропитания повышает удобство его использования (нет необходимости в периодической замене источников электропитания);

- низковольтный двухпроводный интерфейс способствует упрощению монтажа и снижению затрат на него.

К недостаткам метода идентификации с использованием электронных ключей iButton можно отнести:

- открытость протокола обмена данными создает реальную угрозу создания устройств, полностью имитирующих тактику работы электронных ключей iButton (устройства, имитирующие тактику работы электронного ключа DS1990A, уже созданы);

- особенности конструктивного исполнения электронного ключа и его считывателя допускают возможность разрыва электрического соединения в процессе обмена данными, что приводит к появлению ошибок при чтении индивидуального кода;

- контактные поверхности электронного ключа и его считывателя подвержены загрязнению, что может привести к ненадежности

электрического соединения, и, как следствие, к неправильному считыванию индивидуального кода;

– считывающие чашки некоторых конструктивных исполнений не обеспечивают надежного электрического контакта при одновременном использовании ключей iButton, исполненных в версиях F3 и F5.

2.2.4 Бесконтактные идентификаторы RFID

Способ дистанционной (бесконтактной) вещественной идентификации, в английской транскрипции "Proximity", что в буквальном переводе означает "дистанционный". Чтение кода идентификатора происходит на определенном расстоянии от считывателя без непосредственного контакта. Существует несколько технологий записи идентификационного кода на идентификаторы, например, на эффекте поверхностной акустической волны. Однако, наиболее широкое распространение получили идентификаторы с установленной внутри интегральной микросхемой, которая представляет собой достаточно сложное электронное устройство, содержащее в общем случае приемник, передатчик и процессор с памятью в которой храниться идентификационный код. Внутри идентификатора расположена также антенна, с помощью которой происходит обмен данными между считывателем и идентификатором в радиочастотном диапазоне электромагнитных волн. Такой тип дистанционного идентификатора получил название RFID (Radio Frequency IDentification, радиочастотная идентификация). Пример изображения идентификационной RFID карты приведено на рисунке 2.10.

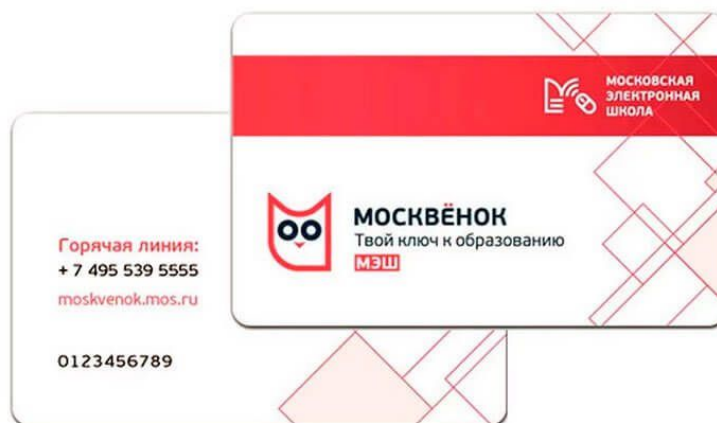


Рисунок 2.10 – Идентификационная RFID карта

По способу обеспечения электропитания RFID идентификаторы подразделяются на:

- пассивные;
- активные;
- полупассивные.

Пассивные RFID идентификаторы не имеют встроенного источника энергии. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования кремниевого чипа, размещенного в метке, и передачи ответного сигнала.

Активные RFID идентификаторы обладают собственным источником электропитания и не зависят от энергии считывателя, вследствие чего они читаются на дальнем расстоянии, имеют большие размеры и могут быть оснащены дополнительной электроникой. Активные RFID идентификаторы обычно имеют гораздо больший радиус считывания и объем памяти чем пассивные и способны хранить больший объем информации для отправки приемопередатчиком.

Полупассивные RFID идентификаторы, также называемые полуактивными, очень похожи на пассивные метки, но оснащены батареей, которая обеспечивает чип энергопитанием.

По типу используемой памяти RFID, идентификаторы подразделяются на:

– RO (англ. Read Only) – данные записываются только один раз, сразу при изготовлении. Такие RFID идентификаторы пригодны только для идентификации. Новую информацию в них записать нельзя и их практически невозможно подделать;

– WORM (англ. Write Once Read Many) – кроме уникального идентификатора такие метки содержат блок однократно записываемой памяти;

– RW (англ. Read and Write) – такие RFID идентификаторы содержат идентификатор и блок памяти для чтения/записи информации. Данные в них могут быть перезаписаны многократно.

Существует четыре диапазона рабочих частот, которые наиболее широко применяются RFID идентификаторами: 125 кГц; 13,56 МГц; 860 – 928 МГц; 2,45 ГГц. Основные технические параметры, характеризующие RFID идентификаторы, использующие каждый из частотных диапазонов, приведены в таблицах 2.2 – 2.5.

Таблица 2.2 – Основные технические параметры, характеризующие RFID идентификаторы с рабочей частотой 125 кГц

125 кГц	
Расстояние считывания	от 3 до 70 см
Скорость передачи данных	до 9600 бит/сек
Наличие антиколлизии	есть, но не у всех
Объем памяти	32 – 1024 байта
Существующие типы считывателей	Стационарные, стационарные с выносной антенной, настенные, ручные, модули
Сфера использования	Применяются в СКУД и для идентификации животных

Таблица 2.3 – Основные технические параметры, характеризующие RFID идентификаторы с рабочей частотой 13,56 кГц

13,56 МГц	
Расстояние считывания	от 3 до 100 см
Скорость передачи данных	до 64 кбит/сек
Наличие антиколлизии	есть
Объем памяти	8 – 16384 байта
Сфера использования	Применяются в СКУД, платежных системах, для идентификации товаров на складах и книг в библиотечных системах

Таблица 2.4 – Основные технические параметры, характеризующие RFID идентификаторы с рабочей частотой 860 – 928 МГц

860 – 928 МГц	
Расстояние считывания	от 10 см до 10 м
Скорость передачи данных	от 128 и более кбит/сек
Наличие антиколлизии	есть, до 150 идентификаторов/сек
Объем памяти	64 – 1024 бит (ISO), 64 или 96 бит (EPC)
Сфера использования	Применяются в системах логистики и учета движения транспорта. Отличительной особенностью является повышенная дальность и высокая скорость чтения

Таблица 2.5 – Основные технические параметры, характеризующие RFID идентификаторы с рабочей частотой 2,45 ГГц

2,45 ГГц	
Расстояние считывания	от 2 до 10 м
Скорость передачи данных	до 128 и более кбит/сек
Наличие антиколлизии	есть
Объем памяти	от 64 бит до 32 кбайт
Сфера использования	Применяются в системах логистики и учета движения транспорта. Отличительной особенностью является повышенная дальность и высокая скорость чтения

Помимо RFID карт, идентификаторы данного типа выполняются в виде брелоков, браслетов, для установки на автотранспортные средства и т.п. Примеры RFID идентификаторов, выполненных в различных исполнениях, приведены на рисунках 2.11 – 2.13.



Рисунок 2.11 – RFID идентификатор в виде брелока



Рисунок 2.12 – RFID идентификатор в виде браслета



Рисунок 2.13 – RFID идентификатор для установки на автотранспортное средство

Расстояние считывания зависит от мощности электромагнитного поля считывателя и от габаритов антенны.

К достоинствам метода идентификации на основе использования бесконтактных идентификаторов RFID можно отнести:

- низкую стоимость идентификаторов и считывателей;
- неконтактный, дистанционный обмен данными между идентификатором и считывателем, обеспечивает наибольшую пропускную способность и является наиболее удобным для пользователей;
- бесконтактное считывание идентификатора позволяет применить скрытую установку считывателя, что значительно повышает устойчивость системы к криминальным воздействиям, вандалоустойчивость и устойчивость к неблагоприятным природным факторам;
- высокая степень устойчивости идентификаторов к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);
- высокие имитостойкость и степень защищенности от несанкционированного копирования, обеспечиваемые наличием кодированного обмена данными;
- большой объем памяти данных, записываемых на идентификатор, позволяет использовать многоразрядные коды, что значительно увеличивает число комбинаций кодов;
- продолжительный срок службы идентификаторов;
- отсутствие в пассивных идентификаторах источника электропитания повышает удобство их использования (нет необходимости в периодической замене источников электропитания). В тоже время наличие в активных идентификаторах встроенного источника электропитания обеспечивает увеличение дальности считывания;
- взаимная ориентация идентификатора и считывателя не имеет принципиального значения;

– бытовые радиопередающие устройства, электронные ключи или брелоки, находящиеся в контакте с идентификатором, не мешают его обмену данными со считывателем.

К недостаткам метода идентификации на основе использования бесконтактных идентификаторов RFID можно отнести:

– из-за использования передачи данных по радиоканалу становится возможным их несанкционированное дистанционное считывание, что при отсутствии криптозащиты протокола обмена данными позволяет злоумышленникам, используя сравнительно несложную аппаратуру, имитировать работу идентификатора;

– одновременное внесение в чувствительную зону считывателя сразу нескольких идентификаторов (возникновение коллизии) может привести к неправильной работе системы.

2.3 Примеры биометрических технологий, применяемых в СКУД

Долгие годы самым распространенным способом биометрической идентификации была дактилоскопия (опознавание личности по отпечатку пальцев рук), что обуславливалось наличием широкой номенклатуры физических принципов считывания (оптический, емкостной, тепловой, ультразвуковой, радиочастотный), применимых для обеспечения различного уровня безопасности и сравнительно малыми габаритами считывателей, что позволяло размещать их в таких устройствах как электронные замки, ноутбуки, смартфоны, флеш-карты и др.

В условиях разразившейся в 2020 году пандемии COVID-19 стало наиболее актуально применение бесконтактных биометрических технологических решений:

- анализ изображения лица;
- анализ рисунка роговицы глаз;
- анализ расположения кровеносных сосудов.

2.3.1 Идентификация по отпечатку пальца

Идентификация по отпечатку пальца построена на двух основных качествах, присущих узорам папиллярных линий пальцев:

стабильность рисунка узора на протяжении всей жизни человека;

уникальность рисунка, что означает отсутствие двух людей с одинаковыми дактилоскопическими отпечатками.

Пример изображения отпечатка пальца человека показан на рисунке 2.14.



Рисунок 2.14 – Отпечаток пальца человека

Внешний вид одного из считывателей отпечатка пальца показан на рисунке 2.15.



Рисунок 2.15 – Считыватель отпечатка пальца

Существует два основных алгоритма сравнения полученного кода с имеющимся в базе шаблоном: по характерным точкам и по рельефу всей поверхности пальца. В первом случае выявляются характерные участки и запоминается их взаиморасположение. Во втором случае запоминается вся "картина" в целом. В современных системах используется также комбинация обоих алгоритмов, что позволяет повысить уровень надежности системы.

Наиболее широко применяются три основных подхода к реализации УС идентификации по отпечаткам пальцев.

Самый распространенный на сегодня способ (оптический) строится на использовании оптики – призмы и нескольких линз со встроенным источником света. Свет, падающий на призму, отражается от поверхности, соприкасающейся с пальцем пользователя, и выходит через другую сторону призмы, попадая на оптический сенсор (обычно, монохромная видеокамера на основе ПЗС-матрицы), где формируется изображение (см. рисунок 2.16).

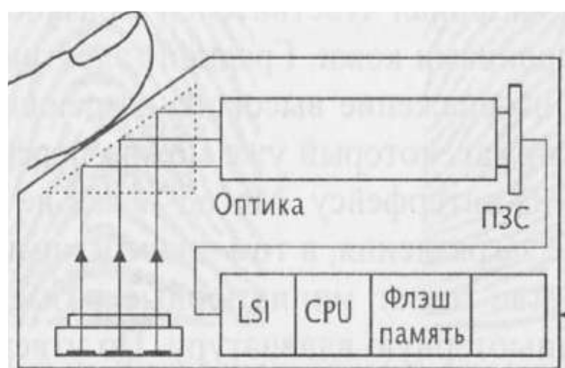


Рисунок 2.16 – Оптический способ реализации УС для идентификации по отпечаткам пальцев

Другой способ (емкостной) использует методику измерения электрического поля пальца с применением полупроводниковой пластины. Когда пользователь устанавливает палец в сенсор, он выступает в качестве одной из пластин конденсатора (см. рисунок 2.17). Другая пластина

конденсатора – это поверхность сенсора, которая состоит из кремниевого чипа, содержащего 90 тысяч конденсаторных пластин с шагом считывания 500 точек на дюйм. В результате получается 8-битовое растровое изображение гребней и впадин пальца.

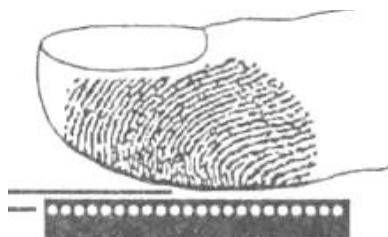


Рисунок 2.17 – Емкостной способ реализации УС для идентификации по отпечаткам пальцев

Еще один способ – ультразвуковое сканирование. Передатчик отправляет ультразвуковой импульс на палец. Одна часть сигнала поглощается, другая возвращается обратно и улавливается приемником. Алгоритм оценивает силу отраженной волны на разных участках сканера и формирует трехмерную копию отпечатка. Достоинством способа является возможность сканирования сильно загрязненных пальцев.

К достоинствам метода идентификации по отпечатку пальца можно отнести:

- низкую стоимость считывателей, сканирующих изображение отпечатка пальца с использованием оптического и емкостного методов сканирования;
- простоту и удобство для пользователя процедуры сканирования отпечатков пальцев.

К недостаткам метода идентификации по отпечатку пальца можно отнести:

- поверхность кожного покрова пальцев часто повреждается из-за оказываемых на руки внешних механических и химических воздействий, что может привести к искажению считываемого биометрического признака – узора папиллярных линий;

– в системах, использующих полупроводниковый и емкостной методы сканирования отпечатка пальцев, возникают проблемы при сканировании пальцев людей, обладающих сухой кожей или при сканировании мокрых пальцев;

– низкую имитостойкость систем, не оснащенных дополнительными средствами распознавания признаков, присущих пальцам живого человека;

– определенным недостатком является исторически сложившееся предубеждение в сознании людей, что снятие отпечатков папиллярных линий пальцев ассоциируется с криминальными целями, а также с вторжением в частную жизнь и это вызывает негативный оттенок в реакции на сканирование отпечатков папиллярных линий пальцев;

– критичность метода идентификации к чистоте сканирующей поверхности считывателя и кожного покрова пальцев.

2.3.2 Идентификация по изображению лица

Для анализа изображения лица используются различные алгоритмические методы, при которых регистрация изображений лица происходит в видимой, ближней инфракрасной или дальней инфракрасной (тепловизионной) области спектра. При этом неоспоримым преимуществом этого вида идентификации является возможность распознавания нескольких десятков лиц в потоке (при движении в толпе).

Широкое распространение получили четыре основных метода распознавания лица, различающихся сложностью реализации и целью применения:

– «Eigenfaces»;

– анализ «отличительных черт»;

– анализ на основе «нейронных сетей»;

– метод «автоматической обработки изображения лица».

«Eigenface» можно перевести как «собственное лицо». Эта технология

использует двумерные изображения в градациях серого, которые представляют отличительные характеристики изображения лица. Метод «Eigenface» часто используется в качестве основы для других методов распознавания лица. В момент регистрации «Eigenface» каждого конкретного человека представляется в виде ряда коэффициентов. Для установления подлинности шаблон, полученный при регистрации, сравнивается с уже ранее зарегистрированным шаблоном с целью определения коэффициента различия. Степень различия между шаблонами определяет факт идентификации. Технология «Eigenface» оптимальна при использовании в хорошо освещенных помещениях, когда есть возможность сканирования лица в фас.

Метод анализа «отличительных черт» подобен методу «Eigenface», но в большей степени адаптирован к изменению внешности или мимики человека (улыбающееся или хмурящееся лицо). В технологии «отличительных черт» используются десятки характерных особенностей различных областей лица, причем с учетом их относительного местоположения. Индивидуальная комбинация этих параметров определяет особенности каждого конкретного лица. Лицо человека уникально, но достаточно динамично, так как человек может улыбаться, отпустить бороду и усы, надеть очки – все это увеличивает сложность процедуры идентификации. Например, при улыбке наблюдается некоторое смещение частей лица, расположенных около рта, что в свою очередь будет вызывать подобное движение смежных частей. Учитывая такие смещения, можно однозначно идентифицировать человека и при различных мимических изменениях лица. Так как этот анализ рассматривает локальные участки лица, допустимые отклонения могут находиться в пределах до 25° в горизонтальной плоскости и приблизительно до 15° в вертикальной плоскости и требует достаточно мощной и дорогой аппаратуры, что соответственно снижает возможности распространения данного метода.

В методе, основанном на нейронной сети, характерные особенности

обоих лиц – зарегистрированного и проверяемого сравниваются на совпадение. «Нейронные сети» используют алгоритм, устанавливающий соответствие уникальных параметров лица проверяемого человека и параметров шаблона, находящегося в базе данных, при этом применяется максимально возможное число параметров. По мере сравнения определяются несоответствия между лицом проверяемого и шаблоном из базы данных, затем запускается механизм, который с помощью соответствующих весовых коэффициентов определяет степень соответствия проверяемого лица шаблону из базы данных. Этот метод увеличивает качество идентификации лица в сложных условиях.

Метод автоматической обработки изображения лица – наиболее простая технология, использующая расстояния и отношение расстояний между легко определяемыми точками лица, такими, как глаза, конец носа, уголки рта. Хотя данный метод не столь мощный, как «eigenfaces» или «нейронная сеть», он может быть достаточно эффективно использован в условиях слабой освещенности.

2.3.3 Идентификация по кровеносным сосудам

Кровеносные сосуды (вены), которые находятся в подкожных областях человеческого тела, формируют уникальный рисунок для каждого человека.

Пример рисунка кровеносных сосудов показан на рисунке 2.18.

Пример считывателя рисунка кровеносных сосудов показан на рисунке 2.19.

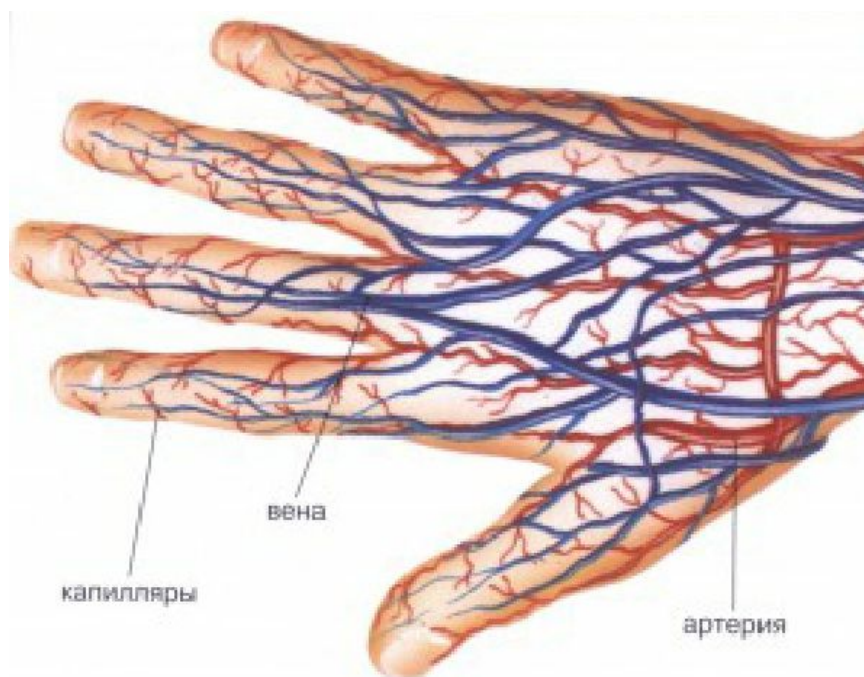


Рисунок 2.18 – Рисунок кровеносных сосудов



Рисунок 2.19 – Считыватель рисунка кровеносных сосудов

Рисунок кровеносных сосудов может быть получен при помощи ИК-излучения, либо напрямую падающего на область, которая должна быть сканирована, либо проходящего через часть тела, изображение которой надо получить. Кровеносные сосуды поглощают ИК-излучение больше,

чем окружающие их ткани, поэтому они выглядят более темными на полученном изображении. Рисунок кровеносных сосудов затем может быть извлечен и преобразован в контрольный биометрический шаблон или зарегистрированный биометрический образец для сравнения в биометрической системе.

В данной технологии выбираются такие части человеческого тела (ладонь, пальцы, запястье и тыльная сторона ладони), в которых присутствует уникальный рисунок кровеносных сосудов, следовательно, биометрический сканер может зарегистрировать эти данные. Дистанция считывания может составлять до десятков сантиметров.

Недостатком метода является то, что УС имеет значительные габариты, сопоставимые с размерами ладони и при сканировании требуется точное позиционирование ладони над УС.

2.3.4 Идентификация по радужной оболочке глаза

Пример изображения радужной оболочки глаза показан на рисунке 2.20.

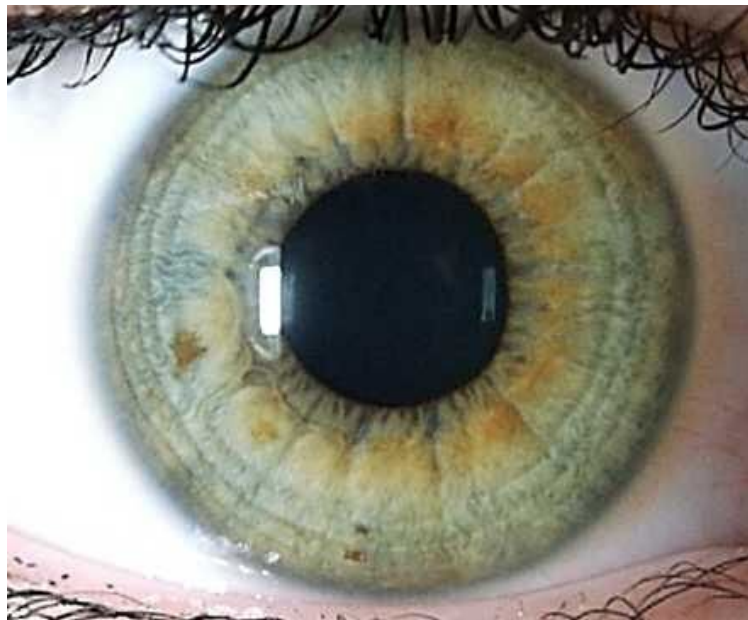


Рисунок 2.20 – Радужная оболочка глаза

В настоящий момент существуют технологии, которые позволяют получать изображения радужной оболочки глаз с расстояния более одного метра или изображения радужной оболочки глаз людей, проходящих через терминал (идентификация в потоке).

Технологии различаются в зависимости от производителя: в некоторых системах получают изображения одного глаза, а в некоторых – обоих глаз одновременно.

В большинстве реализаций изображение РОГ в оттенках серого получают в инфракрасном спектре, чтобы повысить детализацию изображений глаз всех цветов. Для обеспечения сужения зрачка в целях увеличения площади РОГ получение изображения должно осуществляться в хорошо освещенном помещении. Контактные линзы без рисунка и очки несущественно влияют на сбор изображений РОГ.

2.4 Спуфинг и антиспуфинг

Биометрический спуфинг – это метод обмана биометрических УС, путем подмены истинного биометрического признака муляжом.

В качестве одной из возможностей по обману УС отпечатка пальца считается изготовление искусственной кисти с требуемыми отпечатками пальцев (или изъятия «подлинника» у законного владельца).

Для противодействия спуфингу в состав УС могут быть включены:

- инфракрасный детектор, который позволит зафиксировать тепловое излучение от руки (или пальца);

- фотоплетизмограф, который определяет наличие изменений отражения света от поверхности потока крови;

- измеритель электрического сопротивления кожи, который позволит контролировать изменение сопротивления организма при различных воздействиях на человека и различном психофизическом состоянии.

При распознавании лица или при идентификации по РОГ

применяются аппаратные и программные методы антиспуфинга. Аппаратные методы предполагают использование дополнительного оборудования, инфракрасных камер, термальных камер, 3D-камер. Благодаря низкой чувствительности к условиям освещения и способности фиксировать специфические различия в изображениях данные методы считаются наиболее надежными. К недостаткам таких методов можно отнести высокую стоимость дополнительных датчиков и сложность интеграции в существующие системы распознавания лиц.

Существует два типа программных методов: активные (динамические) и пассивные (статические). Активные методы требуют сотрудничества со стороны пользователя. В этом случае система предлагает пользователю выполнить определенные действия в соответствии с инструкцией, например, моргнуть, повернуть голову определенным образом, улыбнуться и т.д. Отсюда проистекают недостатки подобных методов:

во-первых, необходимость сотрудничества нивелирует преимущество системы распознавания лиц, как некооперативного типа биометрической аутентификации, пользователи не очень любят тратить время на лишние «телодвижения»;

во-вторых, если требуемые действия заранее известны, защиту можно обойти путем воспроизведения видео или 3D-репликой с имитацией мимики/движений.

Суть пассивных программных методов в обнаружении движения по последовательности входных кадров для извлечения динамических признаков, позволяющих различать реальные и поддельные лица. Методы анализа основываются на том, что движение плоских 2D-объектов существенно отличается от движения реального человеческого лица, которое представляет собой 3D-объект. Поскольку активные методы используют более чем один кадр, они требуют больше времени на принятие решения. Частота движений лица обычно колеблется от 0,2 до 0,5 Гц.,

поэтому сбор данных для обнаружения спуфинга занимает более 3 секунд.

В настоящее время неизвестны случаи подделки идентификационного признака – рисунка кровеносных сосудов. На данный момент этот метод биометрической идентификации наиболее защищен от спуфинга.

2.5 Мультибиометрия и многофакторные решения

С целью повышения достоверности биометрической идентификации применяют метод мультибиометрических технологий.

Различают следующие технологии:

- анализ различных биометрических характеристик (отпечаток пальца и лицевая биометрия);

- анализ множественных биометрических характеристик (отпечатки различных пальцев, радужная оболочка левого и правого глаза);

- анализ при различных способах получения биометрических образов (лицевая биометрия в видимом и инфракрасном свете);

- анализ при различных типах сканеров (оптический и емкостной для сканирования отпечатков пальцев);

- анализ при повторных образцах одной биометрической характеристики;

- анализ при использовании нескольких различных алгоритмов сравнения биометрических образов.

В многофакторных решениях наряду с биометрической идентификацией используется запоминаемая или вещественная идентификация. Цель многофакторных решений – ускорение процесса опознавания пользователя, а точнее применение метода верификации (сравнение биометрического образа не со всей базой данных, а с конкретным образом, установленным методом запоминаемой или вещественной идентификации).

Примером многофакторного решения может служить

запатентованная технология fingerPIN™.

Особенность данной технологии заключается в том, что, помимо сканирования отпечатков пальцев, от пользователя требуется соблюдать очередность их прикладывания. Например, если пронумеровать пальцы рук от 0 до 9 и потребовать использовать комбинацию из 4 отпечатков, то при обучении будут получаться различные комбинации отпечатков (так называемый био-PIN) 0343,1313, 6789 и т.п.

Данную комбинацию пользователь держит в секрете, что в сумме с его отпечатками позволяет считать такой тип аутентификации двухфакторным.

3 Требования к СКУД физического доступа

СКУД физического доступа должны обеспечивать:

- санкционированный доступ людей, транспорта и других объектов в (из) помещения, здания, зоны и территории, путем идентификации;

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

- СКУД (кроме автономных) должна выполнять следующие основные функции:

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

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

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

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

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

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

- ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при чрезвычайных ситуациях, пожаре, при технических

неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

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

- автоматическое открытие определенных дверей по пожарной тревоге;

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

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

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

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

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

- возможность архивирования базы и просмотра архива в автономном режиме;

- возможность идентификации пользователей СКУД по фотографиям из базы системы при проходе через турникеты (проезде через ворота);

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

- учет пользователей системы по типу пропусков:

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

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

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

3.1 Построение и варианты развертывания СКУД

По архитектурному построению СКУД подразделяют на:

- автономные – для управления одним или несколькими УПУ без передачи информации на центральное устройство управления и контроля со стороны оператора;

- распределенные (одноранговые) – для управления несколькими УПУ, при этом база данных идентификаторов (и событий в системе) содержится в соответствующих контроллерах;

- централизованные (многоранговые) – для управления несколькими УПУ, при этом управление осуществляется с помощью центрального контроллера, в котором и хранится база данных идентификаторов (и событий в системе);

- многоуровневые – для управления несколькими УПУ, при этом управление осуществляется с помощью центрального контроллера в котором и хранится база данных идентификаторов (и событий в системе), взаимодействующего с периферийными контроллерами с собственными буферами памяти в которых хранится база данных соответствующих идентификаторов (и соответствующих периферийных событий);

- кластерные – для управления несколькими УПУ, при этом база данных идентификаторов (и событий в системе) содержится в соответствующих контроллерах, при этом осуществляется прямое взаимодействие между контроллерами, входящими в систему, или выделяется master-контроллер, через которых осуществляется управление системой (всеми остальными slave-контроллерами);

- облачные – для управления несколькими УПУ, при этом база данных идентификаторов (и событий в системе) может содержаться в облаке или в соответствующих контроллерах, при этом взаимодействие между контроллерами входящими в систему может осуществляться посредством облачных технологий;

– смешанные и гибридные – для управления несколькими УПУ, при этом возможны различные сочетания подсистем, входящих в единую СКУД.

По вариантам развертывания СКУД подразделяются на:

– изолированные – при этом все модули ПО (сервер базы данных, ядро, функциональные модули, драйверы устройств и управляющая консоль) устанавливаются в центральном контроллере (компьютере);

– централизованные многопользовательские – при этом все служебные модули ПО (ядро, драйверы устройств и логики) функционируют в центральном контроллере, а запуск управляющей консоли возможен и на иных контроллерах;

– распределенные – при этом сервер управления базой данных и ядро работают на центральном контроллере, а драйверы устройств и логики распределены по всей сети;

– многофилиальные – при этом СКУД представляет собой несколько взаимодействующих филиалов каждый из которых находится под управлением автономного ПО, включающего в себя ядро системы, драйверы устройств и логики, а так же базы данных.

3.2 Требования к средствам КУД

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

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

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.

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

3.2.1 Требования к ИД и УС

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

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

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

Допускается в УС 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.

УС должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды и степень защиты должны быть указаны в соответствующих стандартах и сопроводительных эксплуатационных документах.

УС при взломе и вскрытии, а также в случае обрыва или короткого замыкания, подходящих к ним электрических 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.

Конструкция, внешний вид и надписи на ИД и УС не должны приводить к раскрытию применяемых кодов.

3.2.2 Требования к СУ

Аппаратные средства управления (контроллеры) должны обеспечивать прием информации от УС, обработку информации и выработку сигналов управления на УПУ.

Контроллеры в системах с централизованным управлением 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 электропитания и при переходе на резервное электропитание;

– контроль линий связи между контроллерами, средствами централизованного управления.

Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также, обеспечивать имитостойкость и защиту информации.

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.

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

3.2.3 Требования к УПУ

В УПУ должны входить:

– конструкции преграждающие (КП): подвижные (полотна дверей, турникетов, распашных створок, вращающихся дверей и др.) и неподвижные (например, стены и потолки шлюзов, а также другие элементы конструктивных препятствий, входящие в состав конструкции УПУ конкретного типа);

– устройства исполнительные (УИ): механизмы привода КП различных типов, а также замки и защелки.

УПУ по исполнению КП делят на следующие основные виды:

– УПУ с КП в виде дверных полотен различных видов распашного, складывающегося, раздвижного и вращающегося типов со сплошным перекрытием проема прохода;

– УПУ с КП в виде турникетов с планками или створками всех вышеперечисленных типов с частичным перекрытием проема прохода;

– УПУ с КП в виде турникетов с планками или створками всех вышеперечисленных типов с полным перекрытием проема прохода;

– УПУ с блокированием объекта в точке доступа и с КП в виде дверных полотен и/или планок (створок) всех вышеперечисленных типов, а также комбинациями этих КП в любом сочетании.

Механизмы привода КП, применяемые в УПУ, подразделяют:

– на электромеханические;

– на гидравлические;

– на пневматические.

Замки и защелки, применяемые в УПУ, подразделяют:

– на электромеханические замки;

– на электромагнитные замки;

– на электромагнитные защелки.

В УПУ могут входить средства специального контроля:

– металлообнаружители;

– системы взвешивания;

– рентгеновские устройства досмотра;

– устройства для обнаружения взрывчатых веществ;

– устройства для обнаружения наркотических веществ;

– устройства радиационного контроля;

– другие виды средств специального контроля.

УПУ должны обеспечивать:

– возможность круглосуточной и/или сменной работы в контрольно-пропускном режиме, а также возможность переключения на ручное управление для проведения технического обслуживания по регламенту;

- полное или частичное перекрытие проема при попытке несанкционированного перемещения;

- перемещение людей с установленной пропускной способностью в соответствии с установленным контрольно-пропускным режимом;

- свободное перемещение через УПУ для эвакуации людей и материальных ценностей при чрезвычайных ситуациях;

- возможность блокирования человека в замкнутом пространстве (для шлюзов, кабин с вращающимися дверями и т.д.) при обнаружении несанкционированного прохода;

- контроль нормально открытого или нормально закрытого состояния КП УПУ и световую индикацию этого состояния;

- возможность возврата КП УПУ в закрытое состояние при отсутствии прохода в течение установленного времени;

- необходимые санитарно-гигиенические условия (для шлюзов и т.п.) в замкнутом объеме (воздухообмен по ГОСТ 12.1.005–88, освещение по ГОСТ 12.1.046–2014).

По согласованию с заказчиком УПУ могут обеспечивать:

- защиту от прохода через них одновременно не менее двух человек, если это не предусмотрено контрольно-пропускным режимом;

- возможность подключения дополнительных световых и/или звуковых устройств для подачи сигнала при попытках несанкционированного доступа;

- возможность установки переговорных устройств и/или охранных телевизионных систем для работы совместно с системой КУД;

- возможность подключения звуковых устройств для подачи сигнала при открывании нормально закрытых УПУ.

В УПУ должно быть предусмотрено механическое открывание КП для свободного прохода людей с целью обеспечения их эвакуации при авариях и стихийных бедствиях, а также при технических неисправностях.

При этом следует использовать один из видов разблокировки:

– механическую с обеспечением свободного прохода;

– автоматическую путем выдачи штатной команды «авария» с обеспечением свободного прохода;

– путем выключения электропитания с обеспечением свободного прохода.

Аварийная система разблокировки должна быть защищена от возможности ее использования для несанкционированных действий.

Ширина прохода через УПУ должна быть не менее 600 мм.

Минимальная ширина УПУ для проезда инвалидов в колясках должна составлять не менее 900 мм.

Высота прохода в кабине должна быть не менее 1,9 м.

При монтаже на объекте в отдельных случаях допускается неполное (по ширине проема) перекрытие прохода турникетом.

УПУ, работающие при напряжениях свыше 42 В, должны быть оборудованы заземлением в соответствии с требованиями ГОСТ 12.2.007.0–1975.

Для УПУ, конструкция которых может угрожать безопасности людей при работе УИ (шлюзов и т.п.), положение КП УИ и наличие препятствий в зоне их работы в целях обеспечения безопасности должны контролироваться датчиками (радиоволновыми, инфракрасными, пневматическими и др.).

При работе приводов подъемных УПУ должна быть исключена возможность возникновения опасности для жизни и здоровья человека при самопроизвольном прекращении подачи электроэнергии, а также не должно происходить самопроизвольного изменения состояния этих устройств при восстановлении подачи энергии.

3.3 Требования по защите информации в СКУД

В СКУД должны быть приняты следующие меры по защите информации:

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

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

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

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

- размещение СВТ в отдельных режимных помещениях;
- разделение функций технического обслуживания и ремонта от функций администрирования СКУД;
- периодическая смена паролей.

Перечисленные выше мероприятия дополняются следующими мерами:

- проверкой отсутствия посторонних устройств в составе СКУД;
- защитой аппаратуры от электромагнитного излучения и наводок.

ПО СКУД должно быть защищено от несанкционированного доступа с помощью паролей с разделением по типу пользователей:

- первый тип («администратор») – доступ ко всем функциям ПО СКУД;

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

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

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

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

3.4 Требования надежности

В ТУ на средства и системы КУД должны быть установлены следующие показатели надежности в соответствии с ГОСТ 27.002–2015 и ГОСТ 27.003–2016:

- 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.

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

Средний срок службы систем КУД должен быть не менее восьми лет с учетом проведения технического обслуживания и ремонтно-восстановительных работ.

3.5 Требования электромагнитной совместимости

Средства КУД, в зависимости от области применения и условий эксплуатации, должны обеспечивать помехоустойчивость при воздействии электромагнитных помех следующих степеней жесткости по ГОСТ Р 50009-2000:

– второй степени жесткости – для эксплуатации в закрытых помещениях;

– третьей степени жесткости – для эксплуатации на открытых площадках и периметрах территорий.

Уровни промышленных радиопомех, создаваемых УПУ, должны соответствовать нормам по ГОСТ Р 50009-2000.

3.6 Требования безопасности

Средства КУД должны удовлетворять общим требованиям безопасности, установленным в ГОСТ Р 52435–2015.

Конструктивное исполнение средств КУД должно обеспечивать их пожарную безопасность по ГОСТ ИЕС 60065–2013 в аварийном режиме работы и при нарушении правил эксплуатации.

Значения электрической прочности изоляции средств КУД должны соответствовать требованиям ГОСТ Р 52931-2008.

Значения электрического сопротивления изоляции цепей средств

КУД должны соответствовать требованиям ГОСТ Р 52931–2008.

Средства КУД, предназначенные для эксплуатации в зонах с взрывоопасной средой, должны соответствовать требованиям Технического регламента таможенного союза ТР ТС 012/2011 «О безопасности оборудования для работы во взрывоопасных средах».

3.7 Требования устойчивости к климатическим и механическим воздействиям

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

3.8 Требования к электропитанию

Электропитание средств КУД допускается осуществлять от:

- однофазной электрической сети переменного тока напряжением 230 В частотой 50 Гц по ГОСТ 29322–2014;
- ИЭПВР по ГОСТ Р 53560–2022;
- других средств КУД, имеющих специально предназначенные для этого выходы;
- автономных источников электропитания.

Средства КУД, электропитание которых осуществляется от однофазной электрической сети переменного тока номинальным напряжением 230 В (по ГОСТ 29322-2014), должны:

- иметь возможность подключения внешней АКБ;
- сохранять работоспособность при отклонении напряжения

электропитания от номинального значения в пределах от минус 20 % до плюс 10 %;

– обеспечивать функционирование в режимах, при которых ток потребления достигает максимального значения (с учетом максимальной допустимой нагрузки выходных цепей) без использования энергии АКБ.

Средства КУД, электропитание которых осуществляется от ИЭПВР, должны сохранять работоспособность при отклонении напряжения электропитания от номинального значения напряжения (12 В или 24 В) на ± 15 %.

3.9 Требования к технической документации

Эксплуатационные документы должны быть выполнены в соответствии с требованиями ГОСТ 2.601-2019, ГОСТ 2.610-2019, содержать все необходимые сведения для проведения монтажных и пуско-наладочных работ, эксплуатации, технического обслуживания СКУД.

Эксплуатационные документы должны поставляться в комплекте со средствами КУД.

Допускается размещение эксплуатационных документов (кроме формуляра, паспорта или этикетки, в которых содержатся сведения о дате выпуска, приемке и упаковке, заверенные штампом предприятия-изготовителя) на электронных носителях информации или в информационно-коммуникационной сети общего пользования (на сайте предприятия-изготовителя в сети Интернет).

4 Выбор СКУД для оборудования объекта

4.1 Принципы выбора СКУД для объекта

В основе принципа выбора СКУД должно лежать достижение максимальной эффективности выполнения задач, стоящих перед СКУД.

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

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

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

- третья зона – специальные помещения объекта, доступ в которые имеют строго определенный персонал.

Пропуск работников на объект через точки доступа должен осуществляться:

- в первой зоне доступа по одному признаку идентификации;

- во второй зоне доступа – по двум признакам идентификации (например, запоминаемая (код) и вещественная идентификация (электронная карточка) или вещественная и биометрическая идентификация);

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

СКУД рекомендуется оборудовать:

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

- турникеты входов в здание;
- кабинеты руководства (входы на VIP-этаж);
- двери выходов из лифтовых холлов;
- служебные входы;
- помещения охраны;
- помещения, в которых непосредственно сосредоточены материальные ценности;
- режимные помещения и зоны ограниченного доступа (АТС, серверные, кроссовые, аппаратные, диспетчерские пункты, помещения жизнеобеспечения здания и т.п.);
- помещения, согласованные с руководителем объекта дополнительно в ходе проектирования.

СКУД должна содержать следующие АРМ:

- АРМ администратора;
- АРМ дежурного оператора охраны;
- АРМ оператора на проходной;
- АРМ бюро пропусков;
- АРМ отдела кадров.

Функции отдельных АРМ СКУД могут объединяться на одном рабочем месте.

4.2 Принципы построения СКУД объекта

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

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

– адаптивности.

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

Зональный принцип: СКУД объекта должна предусматривать возможность создание отдельных зон ограниченного доступа.

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

Принцип равнопрочности: требуемый уровень эффективности СКУД должен быть обеспечен для всех видов криминальных угроз (несанкционированного проникновения), выявленных в процессе анализа уязвимости объекта.

Требуемый уровень эффективности защиты должен учитывать особенности критических элементов и критерия «эффективность/стоимость».

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

4.3 Обследование объекта

Выбор варианта оборудования объекта СКУД следует начинать с его обследования.

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.);
- материалы строительных конструкций;
- количество отдельно стоящих зданий, их этажность;
- количество открытых площадок;
- количество отапливаемых и неотапливаемых помещений и их расположение;
- наличие и особенности работы штатных инженерно-технических коммуникаций;
- условия эксплуатации и режимы работы помещений;
- ограничения или расширения права доступа отдельных сотрудников.

При наличии агрессивных условий эксплуатации: вне закрытых отапливаемых помещений, помещений с повышенным содержанием пыли, влажности воздуха, низкой температурой, следует ориентироваться на специализированные средства КУД, предназначенные для работы в особых условиях.

Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения электропитания, удаленность компонентов от управляющего центра, заземление средств КУД и т. п.

По результатам обследования определяются структура, функциональные и необходимые тактико-технические характеристики, составляется задание на оборудование объекта.

В техническом задании указываются:

- назначение СКУД, техническое обоснование и описание системы;
- виды идентификации, применяемые в СКУД;
- размещение средств КУД;
- условия эксплуатации средств КУД;
- основные технические характеристики средств КУД;
- требования к маскировке и защите средств КУД от вандализма;
- требования к оповещению о тревожных и аварийных ситуациях;
- требования к безопасности;
- требования к электропитанию;
- требования к обслуживанию и ремонту СКУД;
- требования к возможности включения СКУД в ИСБ объекта;
- пропускная способность в охраняемые зоны особенно в час-пик;
- максимально возможное число пользователей на одно УС;
- алгоритм работы СКУД в аварийных и чрезвычайных ситуациях.

5 Проектирование СКУД объекта

Проектирование СКУД включает следующие этапы работ:

- проведение анализа уязвимости объекта, оценка эффективности существующей системы (для действующих объектов);
- разработка и утверждение технического задания на проектирование (реконструкцию) СКУД объекта;
- разработка и утверждение проектной документации.

Анализ уязвимости объекта и оценка эффективности, существующей СКУД осуществляется путем проведения комиссионного обследования объекта комиссией, формируемой заказчиком СКУД.

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

- анализ возможных криминальных угроз;
- функциональные и строительные особенности объекта, характер и условия размещения материальных ценностей, радиоактивных, пожаровзрывоопасных и биологических веществ, создающих реальную угрозу возникновения источника кризисной ситуации;
- вид охраны: постовая, техническая, совмещенная (постовая и техническая);
- уязвимые места и строительные конструкции, через которые возможно несанкционированное проникновение на объект;
- зоны доступа, средства КУД, подлежащие монтажу, места их установки и меры по маскировке, способы блокировки строительных конструкций и уязвимых мест.

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

Техническое задание на проектирование СКУД разрабатывается заказчиком СКУД или организацией, уполномоченной на проведение данного вида работ в соответствии с действующим законодательством.

К техническому заданию прилагается:

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

- схема дорог для определения маршрутов движения автотранспорта по территории объекта;

- исходные данные для проектирования в составе:

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

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

- технические условия на подключение электронагрузок проектируемой системы.

Проектная документация должна содержать следующий комплект документов:

- техническое задание на разработку проекта;

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

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

- спецификации оборудования и материалов;

- сметную документацию;

- чертежи не стандартизованного оборудования или задания на его разработку;

- эксплуатационную документацию на СКУД объекта;
- эксплуатационную документацию на средства КУД, входящие в состав СКУД объекта.

Проектная документация согласовывается с заказчиком СКУД.

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

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

6 Размещение технических средств СКУД на объекте

6.1 Устройства центрального управления

Устройства центрального управления 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 защищаются секретными кодами.

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

При объединении компьютеров в сеть целесообразно разделять функциональные возможности среди пользователей сети.

6.2 Устройства контроля и управления

Ведущие контроллеры и контроллеры (СУ), работающие на несколько УПУ 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, 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 электропитания, от которого одновременно питается УПУ с большой индуктивностью обмоток, приводящее к броску напряжения по цепи питания. Для исключения этих нежелательных последствий необходимо предусматривать установку специальных демпфирующих устройств или элементов, гасящих импульсные помехи, вызванные э.д.с. самоиндукции обмотки УПУ.

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.

6.3 Устройства считывающие и устройства преграждающие управляемые

В зависимости от УС и УПУ, 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.

УС карт «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 использовании схематических графических указателей на внешней стороне двери). При монтаже считывателя на металле рекомендуется, чтобы между основанием считывателя и металлической поверхностью расстояние было не менее 25 мм, либо использовать диэлектрическую подложку. 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.

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

УС 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 электро-магнитные 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 нагруженности (до 100 – 200 проходов в день). Применение этих замков для дверей с высокой нагруженностью неэффективно по причине высокого механического износа и как следствие снижения надежности и срока службы.

Электромагнитные замки рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг в условиях высокой нагруженности (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.

7 Ввод в эксплуатацию СКУД

Прием СКУД в эксплуатацию производится рабочей комиссией, в которую включаются представители:

- заказчика СКУД;
- службы охраны объекта;
- монтажной и наладочной организации;
- подразделения вневедомственной охраны войск национальной гвардии Российской Федерации, осуществляющего охрану объекта (по согласованию);

– при необходимости могут быть привлечены специалисты других организаций и ведомств (по согласованию).

При приемке выполненных работ по монтажу и наладке СКУД рабочая комиссия осуществляет:

- проверку качества выполненных монтажных и наладочных работ и их соответствие проектной документации или техническому заданию;
- испытания работоспособности, смонтированной СКУД на соответствие требованиям технического задания.

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

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

- оборудование объекта средствами СКУД выполнено в соответствии с проектной документацией или техническим заданием;
- испытания работоспособности СКУД дали положительные результаты.

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

Основные задачи технического обслуживания СКУД:

- обеспечение бесперебойного функционирования;
- контроль технического состояния СКУД и определение пригодности к дальнейшей эксплуатации;
- выявление и устранение неисправностей и их причин;
- ликвидация или недопущение последствий воздействия климатических, производственных и иных факторов, которые могут отрицательно повлиять на эксплуатационные параметры СКУД.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аналитический обзор «Исследование современных методов персональной идентификации в целях применения в системах централизованного наблюдения» Отчет по НИР. Архив ФКУ «НИЦ «Охрана» Росгвардии, – Москва, 2015, с.102.

2. Андрей Хрулев. Антиспуфинг: как системы распознавания лиц противостоят мошенникам?» (Электронный ресурс) <https://habr.com/ru/companies/speechpro/articles/436700/> (Дата обращения 11.01.2024).

3. ГОСТ 12.1.005-1988 «Общие санитарно-гигиенические требования к воздуху рабочей зоны».

4. ГОСТ 12.1.046-2014 «Строительство. Нормы освещения строительных площадок».

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

6. ГОСТ Р 54831-2011 «Устройства преграждающие управляемые. Общие технические требования. Методы испытаний».

7. «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности Р 78.36.018 – 2021» Методические рекомендации. – Москва: ФКУ «НИЦ «Охрана» Росгвардии, 2022, с. 96.